

H3

Attorney Docket No. 1341.1102CIP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

11017 U.S. PRO  
10/087807  
03/05/02



In re Patent Application of:

Masashi MITOMO, et al.

Application No.:

Group Art Unit:

Filed: February 28, 2002

Examiner:

For: FILTERING APPARATUS, FILTERING METHOD AND COMPUTER PRODUCT

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application Nos. 2001-388444 and 2001-071214

Filed: December 20, 2001 and March 13, 2001, respectively.

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Date: February 28, 2002

Respectfully submitted,  
  
STAAS & HALSEY LLP  
By: \_\_\_\_\_  
James D. Halsey, Jr.  
Registration No. 22,729

700 11th Street, N.W., Ste. 500  
Washington, D.C. 20001  
(202) 434-1500

J1017 U.S. PRO  
10/087807  
03/05/02



日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2001年12月20日

出願番号

Application Number:

特願2001-388444

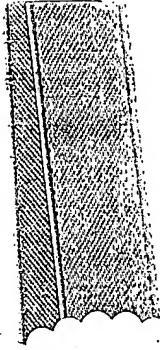
[ST.10/C]:

[JP2001-388444]

出願人

Applicant(s):

富士通株式会社

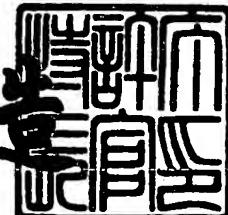


CERTIFIED COPY OF  
PRIORITY DOCUMENT

2002年 1月18日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3117351

【書類名】 特許願  
【整理番号】 0152846  
【提出日】 平成13年12月20日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 15/00  
G06F 13/00  
【発明の名称】 フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム  
【請求項の数】 9  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 三友 仁史  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 鳥居 悟  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 小谷 誠剛  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 滝沢 文恵  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 小野 越夫

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内

【氏名】 小谷野 修

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089118

【弁理士】

【氏名又は名称】 酒井 宏明

【先の出願に基づく優先権主張】

【出願番号】 特願2001- 71214

【出願日】 平成13年 3月13日

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9717671

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【特許請求の範囲】

【請求項1】 クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積手段と、

前記見積手段による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定手段と、

を備えたことを特徴とするフィルタリング装置。

【請求項2】 前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定手段は、前記見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする請求項1に記載のフィルタリング装置。

【請求項3】 前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定手段は、前記見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする請求項1に記載のフィルタリング装置。

【請求項4】 前記サーバに対する正当アクセスのパターンを格納した正当

パターンデータベースと、前記見積手段による正当性の見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする請求項1、2または3に記載のフィルタリング装置。

【請求項5】 所定の外部送信ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信手段をさらに備えたことを特徴とする請求項1～4のいずれか一つに記載のフィルタリング装置。

【請求項6】 所定の格納ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納手段をさらに備えたことを特徴とする請求項1～5のいずれか一つに記載のフィルタリング装置。

【請求項7】 所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新手段をさらに備えたことを特徴とする請求項1～6のいずれか一つに記載のフィルタリング装置。

【請求項8】 クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス要求のみを受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

を含んだことを特徴とするフィルタリング方法。

【請求項9】 クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス

要求のみを受け渡すフィルタリング方法をコンピュータに実行させるプログラムにおいて、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

をコンピュータに実行させるプログラム。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

この発明は、クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムに関する。

##### 【0002】

近時、ネットワーク技術の進展に伴って、インターネット上の分散システムであるWWW (World Wide Web) の利用が急速に拡大し、クライアントからの各種のリクエスト（アクセス要求）に応じて各種のサービスを提供する各種HTTPサーバも累増してきたが、かかるサーバの累増にともなって、クライアントによるサーバへの不正アクセスも増加しつつある。

##### 【0003】

すなわち、侵入者（イントルーダ）や攻撃者（アッカ）が企業、団体、個人などのサーバを無権限で不正に利用したり、運用を妨害したり、破壊（クラック）など、サーバを利用する者がその者に与えられた権限により許された行為以外の行為をネットワークを介して意図的におこなうという不正アクセスが増加している。このため、サーバに対する不正アクセスを拒絶することによりサーバの信頼性を確保する必要性が高まりつつある。

##### 【0004】

### 【従来の技術】

従来より、クライアントによる不正アクセスからサーバを守るために、インターネットと企業LAN（Local Area Network）との間にファイアウォール（Fire Wall）を構築することが一般的におこなわれている。

#### 【0005】

このファイアウォールは、インターネットに接続したコンピュータやネットワークへの外部からの侵入を防ぐためのソフトウェアであり、企業LANとインターネットの間に、特定のデータやプロトコルだけを通すように設計されたファイアウォール用のコンピュータを置き、LAN内と外部とのデータ交換はすべてこのマシンを通しておこなうことにより、外部からの侵入を防ぐというものである。

#### 【0006】

また、このファイアウォールに関連して、ネットワークベースあるいはホストベースの不正アクセス検知手法がある。前者のネットワークベースの不正アクセス検知手法は、ネットワークを流れる生のパケットを監視することにより不正アクセスを発見するものであり、後者のホストベースの不正アクセス検知手法は、ホストに蓄えられたログ履歴を監視することにより不正アクセスを発見するものである。

#### 【0007】

そして、このような不正アクセス検知手法により発見された不正アクセスに基づいて不正アクセスの送信元クライアントを突き止め、この不正アクセスをおこなったクライアントのIPアドレスなどの送信元情報をファイアウォール用のコンピュータ内に蓄積することにより、この送信元情報を含んだクライアントからのアクセス要求を不正アクセスとして拒絶することがファイアウォールにおいて一般的におこなわれている。

#### 【0008】

### 【発明が解決しようとする課題】

しかしながら、上記の従来技術は、過去に不正アクセスをおこなったクライアントを不正クライアントと認定し、この不正クライアントからのアクセス要求を不正アクセスとして拒絶するものであるため、不正クライアントと認定された後

の不正アクセスに対してはサーバを防御することができるが、不正クライアントと認定されていないクライアントからの不正アクセスに対してはサーバを防御することができないという問題点があった。すなわち、不正クライアントと認定される前の初回の不正アクセスに対してはサーバを防御することができない。

#### 【0009】

このため、不正クライアントと認定されていないクライアントからの不正アクセスに対していかにサーバを防御するかが極めて重要な課題となっており、望ましくは、アクセス要求の送信元情報を考慮することなく、正当なアクセス要求であるか不正なアクセス要求であるか否かを判定する枠組みが必要とされている。

#### 【0010】

そこで、この発明は、上述した従来技術による問題点を解消するためになされたものであり、不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができるフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムを提供することを目的とする。

#### 【0011】

##### 【課題を解決するための手段】

上述した課題を解決し、目的を達成するため、請求項1、8または9の発明によれば、図1に示す見積部32は、Webサーバ40に対する不正アクセスのパターンを格納した不正リクエストDB（データベース）33を参照し、不正アクセスのパターンおよび所定の見積ルール32aに基づいてクライアント装置10からのアクセス要求の正当性を見積もり、判定部34は、見積部32による見積結果および所定の判定ルール34aに基づいてアクセス要求をWebサーバ40に受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみをWebサーバ40に受け渡すことができ、もって不正クライアントと認定されていないクライアント装置10からの不正アクセスに対してもWebサーバ40を防御することができる。

## 【0012】

また、請求項2の発明によれば、図1に示す見積部32は、クライアント装置10からのアクセス要求が不正リクエストDB33に格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、クライアント装置10からのアクセス要求が不正リクエストDB33に格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、判定部34は、見積部32により不正アクセスである旨が見積もられたアクセス要求をWebサーバ40に受け渡さないものと判定するとともに、見積部32により正当アクセスである旨が見積もられたアクセス要求をWebサーバ40に受け渡すものと判定することとしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアント装置10からの不正アクセスに対しても迅速かつ確実にWebサーバ40を防御することができる。

## 【0013】

また、請求項3の発明によれば、図1に示す見積部32は、クライアント装置10からのアクセス要求が不正リクエストDB33に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、判定部34は、見積部32により算出された見積値と所定の閾値とを比較してアクセス要求をWebサーバ40に受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアント装置10からの不正アクセスに対してもある程度の幅を持ってWebサーバ40を防御することができる。

## 【0014】

また、請求項4の発明によれば、図5に示す事前判定部71は、見積部32による正当性の見積もりの前に、Webサーバ40に対する正当アクセスのパターンを格納した正当リクエストDB72を参照し、クライアント装置10からのアクセス要求が正当リクエストDB72に格納された正当アクセスのパターンのい

ずれかに該当するか否かを判定し、見積部32は、事前判定部71により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくWebサーバ40に受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

#### 【0015】

また、請求項5の発明によれば、図1に示す外部通報部37は、所定の通報ルール37aに基づいて、判定部34によりWebサーバ40に受け渡さないものと判定されたアクセス要求を所定の外部装置50に送信することとしたので、不正アクセスに関する情報をWebサーバ40の管理者、リクエストフィルタ30の管理者、サーバ装置20全体の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に通報することができ、もってかかる管理者に対しWebサーバ40の保全対策を迅速に促すことができる。

#### 【0016】

また、請求項6の発明によれば、図1に示すログ管理部36は、所定の管理ルール36aに基づいて、判定部34によりWebサーバ40に受け渡さないものと判定されたアクセス要求を所定の格納媒体36bに格納することとしたので、格納媒体36bに格納された不正アクセスに関する情報を分析することなどができる、もってWebサーバ40の更なる保全対策を講じることができる。

#### 【0017】

また、請求項7の発明によれば、図1に示す更新部39は、所定の更新ルール39aに基づいて、不正リクエストDB33、正当リクエストDB72（図5に示す）、見積ルール32a、判定ルール34a、通報ルール37a、管理ルール36aまたは更新ルール39aを更新することとしたので、新たに発見された不正アクセスのパターンを不正リクエストDB33に登録することなどができる、もって日々進化する不正アクセスに対して機動的に対応することができる。

#### 【0018】

## 【発明の実施の形態】

以下に添付図面を参照して、この発明に係るフィルタリング装置、フィルタリング方法、およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。なお、以下に示す実施の形態1～3では、本発明に係るフィルタリング技術を、クライアント装置からのH T T P (HyperText Transfer protocol) リクエストに応じてサービスを提供するサーバ装置に適用した場合について説明する。

## 【0019】

## (実施の形態1)

本実施の形態1では、クライアント装置からのH T T P リクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明する。

## 【0020】

## (1) システムの全体構成

まず最初に、本実施の形態1に係るサーバクライアントシステムの構成について説明する。図1は、本実施の形態1に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態1に係るサーバクライアントシステムは、Webブラウザ11をそれぞれ有する複数のクライアント装置10と、フィルタリング装置としてのリクエストフィルタ30およびWebサーバ40を有するサーバ装置20とを、インターネットなどのネットワーク1を介して相互に通信可能に接続して構成される。

## 【0021】

概略的に、このサーバクライアントシステムにあっては、クライアント装置10は、Webブラウザ11によりサーバ装置20に対してH T T P リクエストなどの各種の処理要求をおこない、サーバ装置20のWebサーバ40は、クライアント装置10からのH T T P リクエストに応じたサービスをクライアント装置10に提供する。そして、サーバ装置20のリクエストフィルタ30は、クライアント装置10とWebサーバ40との間に介在し、クライアント装置10からのH T T P リクエストのうちの正当なリクエストのみをWebサーバ40に受け

渡す。

### 【0022】

ここで、本実施の形態1に係るサーバクライアントシステムは、サーバ装置20のリクエストフィルタ30によるフィルタリング処理に特徴があり、具体的には、リクエストフィルタ30の見積部32は、クライアント装置10からのHTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンのいずれかに該当する場合には不正アクセスである旨を見積もり、判定部34は、見積部32により不正アクセスである旨が見積もられたHTTPリクエストをWebサーバ40に受け渡さないものと判定することにより、HTTPリクエストの送信元情報を問題とすることなく、正当なHTTPリクエストのみをWebサーバ40に受け渡すことができるよう構成している。

### 【0023】

#### (2) クライアント装置の構成

次に、図1に示したクライアント装置10の構成について説明する。同図に示すように、クライアント装置10は、Webブラウザ11を備え、基本的には、サーバ装置20に対してHTTPリクエストなどの処理要求をおこない、サーバ装置20のWebサーバ40により提供されるWebデータを解釈して、モニタなどの出力部に表示させる表示制御（ブラウズ処理）をおこなう。

### 【0024】

そして、このクライアント装置10は、悪意を持った使用方法によってサーバ装置20に対して不正アクセスをおこなうことができる装置でもある。すなわち、クライアント装置10は、侵入者（イントルーダ）や攻撃者（アッカ）などの悪意を持ったユーザの使用によっては、Webサーバ40上のパスワードファイルなどのリモートユーザが見るべきでないファイルを見たり、Webサーバ40上に存在しないファイルをリクエストしてWebサーバ40の機能を停止させたり、コマンド文字列を含んだリクエストによりWebサーバ40上で任意のシステムコマンドを実行するなどの不正アクセスをおこない得るものである。このようなクライアント装置10による不正アクセスに対してWebサーバ40を防御するのがリクエストフィルタ30の役割である。

## 【0025】

なお、クライアント装置10は、たとえば、パーソナルコンピュータやワークステーション、家庭用ゲーム機、インターネットTV、PDA(Personal Digital Assistant)、あるいは、携帯電話やPHS(Personal Handy Phone System)の如き移動体通信端末によって実現することができる。また、クライアント装置10は、モデム、TA、ルータなどの通信装置と電話回線を介して、あるいは、専用線を介して、ネットワーク1に接続されており、所定の通信規約(たとえば、TCP/IPインターネットプロトコル)に従ってサーバ装置20にアクセスすることができる。

## 【0026】

## (3) サーバ装置におけるWebサーバの構成

次に、図1に示したサーバ装置20におけるWebサーバ40の構成について説明する。同図に示すように、サーバ装置20のWebサーバ40は、リクエストフィルタ30を介してクライアント装置10からのHTTPリクエストを受信し、このHTTPリクエストに応じてHTML(HyperText Markup Language)などのマークアップ言語により記述された各種の情報を送信するなどのサービスをクライアント装置10に提供する。

## 【0027】

このWebサーバ40は、機能概念的には、一般的なWebサーバと同様の動作をおこなうものであるが、ここでのWebサーバ40は、一般的なWebサーバと異なり、サーバ装置20においてHTTPリクエストに割り当てられるポート番号80のTCP(Transmission Control Protocol)ポートを監視することはおこなわない。

## 【0028】

すなわち、クライアント装置10からのHTTPリクエストをWebサーバ40により直接に受信するのではなく、リクエストフィルタ30がHTTPリクエストを受信し、プロセス間通信をおこなって正当なHTTPリクエストのみをWebサーバ40に受け渡すこととしている。

## 【0029】

## (4) サーバ装置におけるリクエストフィルタの構成

次に、図1に示したサーバ装置20におけるリクエストフィルタ30の構成について説明する。同図に示すように、リクエストフィルタ30は、受信部31と、見積部32と、不正リクエストDB33と、判定部34と、送信部35と、ログ管理部36と、外部通報部37と、外部情報取得部38と、更新部39とを備える。

## 【0030】

このうち、受信部31は、サーバ装置20におけるポート番号80のTCPポートを監視して、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する処理部である。なお、受信部31によりクライアント装置10から受信したHTTPリクエストは、見積部32および送信部35に出力される。

## 【0031】

見積部32は、不正リクエストDB33に格納された不正アクセスのパターンおよび所定の見積ルール32aに基づいてHTTPリクエストの正当性を見積もり、その見積結果を判定部34に出力する処理部である。

## 【0032】

ここで、見積部32が見積もりに際して参照する不正リクエストDB33について説明する。図2は、不正リクエストDB33に格納される情報の構成例を示す図である。同図に示すように、不正リクエストDB33は、サーバに対する不正アクセスのパターンを格納したデータベースであり、ネットワーク世界で収集された不正アクセスを図示のような形式言語を用いて記述した複数のパターンを記憶している。

## 【0033】

例えば、同図に示す「URL=<//>」のパターンは、URL (Uniform Resource Locator) の先頭が「//」である不正リクエストを意味し、「CGI==phf、ARG=<Qname=root%OA」のパターンは、CGI (Common Gateway Interface) 名が「phf」であり、そのある引数の先頭が「Qname=root%OA」である不正リクエストを意味し、「URL<>..

¥.. ¥.. ¥..」のパターンは、URLに「.. ¥.. ¥.. ¥..」が含まれる不正リクエストを意味し、「CGI>=. htr」のパターンは、CGI名の末尾が「. htr」である不正リクエストを意味する。

#### 【0034】

なお、図2には示していないが、不正リクエストDB33には、Webサーバ40上で任意のシステムコマンドを実行するような不正なコマンド文字列も複数記憶されている。このようなコマンド文字列のパターンを記憶することにより、攻撃方法が既知である不正アクセスだけでなく、攻撃方法が未知である不正アクセスに対してもWebサーバ40を防御することができる。

#### 【0035】

このような不正リクエストDB33を参照することにより、見積部32は、所定の見積ルール32aに基づいてHTTPリクエストの正当性の見積もりをおこなう。具体的には、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンのいずれかに該当する場合には、該HTTPリクエストは不正アクセスである旨を見積もり、一方、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンのいずれにも該当しない場合には、該HTTPリクエストは正当アクセスである旨を見積もる。

#### 【0036】

図1の説明に戻ると、判定部34は、見積部32から受け取った見積結果および所定の判定ルール34aに基づいてHTTPリクエストをWebサーバ40に受け渡すか否かを判定し、この判定結果を送信部35に出力する処理部である。具体的には、見積部32から不正アクセスである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡さないものと判定し（不可判定）、一方、見積部32から正当アクセスである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡すものと判定する（可判定）。

#### 【0037】

送信部35は、判定部34から受け取った判定結果に基づいて、受信部31から受け取ったHTTPリクエストの送信を制御する処理部である。具体的には、

判定部34から可判定を受け取った場合には、HTTPリクエストをプロセス間通信によりWebサーバ40に受け渡す。一方、判定部34から不可判定を受け取った場合には、HTTPリクエストのWebサーバ40への受け渡しを拒絶して、この不正リクエストを破棄する。

#### 【0038】

ログ管理部36は、所定の管理ルール36aに基づいて、判定部34によりWebサーバ40に受け渡さないものと判定された不正リクエストに係る情報を格納媒体36bに格納して管理する処理部である。具体的には、管理ルール36aに基づいて、不正リクエストの内容、送信元情報（IPアドレスやホスト名）、送信時刻、見積部32による見積結果の根拠、判定部34による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に格納媒体36bに格納する。例えば、攻撃性の高い不正リクエストのみを格納するなどである。

#### 【0039】

なお、格納媒体36bに格納された情報は、該格納媒体36bを取り出すことや通信回線を介すことなどによりサーバ装置20の外部に出力することができ、さらに、格納媒体36bに格納された情報を分析して不正アクセスの傾向などを解析することにより、Webサーバ40の更なる保全のために対策を講じることもできる。

#### 【0040】

外部通報部37は、所定の通報ルール37aに基づいて、判定部34によりWebサーバ40に受け渡さないものと判定された不正リクエストに係る情報を外部装置50に通報する処理部である。具体的には、ログ管理部36による処理と同様、通報ルール37aに基づいて、不正リクエストの内容、送信元情報（IPアドレスやホスト名）、送信時刻、見積部32による見積結果の根拠、判定部34による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に外部装置50に通報する。

#### 【0041】

この外部通報部37から通報を受ける外部装置50は、Webサーバ40の管理者、リクエストフィルタ30の管理者、サーバ装置20全体の管理者、ネットワーク全般を監視する公的な機関（管理センタ）の管理者など（以下、これらを総称して「管理者」という。）が操作する通信装置である。そして、外部通報部37は、例えば、攻撃性の高い不正リクエストについてはリアルタイムで迅速に管理者に通報し、攻撃性の低い不正リクエストについては非リアルタイムで一括して管理者に通報するなどして、かかる通報を受ける管理者に対してWebサーバ40の保全対策を迅速に促すことができる。

#### 【0042】

外部情報取得部38は、所定の取得ルール38aに基づいて、更新部39による更新処理に用いられる情報を、外部装置50やWebサーバ40などのリクエストフィルタ30の外部から能動的または受動的に取得する処理部である。例えば、管理者が外部装置50を介して入力した新たな不正リクエストのパターンや、管理者が外部装置50を介して入力した見積ルール32aの変更指示情報などを取得するほか、不正リクエストによる被害を受けたWebサーバ40から被害の状況や不正アクセスの内容などの情報を取得する。なお、所定の取得ルール38aは、権限が認証された管理者からの情報のみを取得するなどの規則である。

#### 【0043】

更新部39は、所定の更新ルール39aに基づいて、不正リクエストDB33、見積ルール32a、判定ルール34a、管理ルール36a、通報ルール37a、取得ルール38aまたは更新ルール39aに格納された情報を更新する処理部である。例えば、外部情報取得部38から新たな不正リクエストのパターンを受け付けた場合には、この不正リクエストのパターンを不正リクエストDB33に格納し、また見積ルール32aの変更指示情報を受け付けた場合には、この変更指示情報に応じて見積ルール32aを変更する。このような更新処理をおこなうことにより、日々進化する不正アクセスに対して機動的に対応することができる

#### 【0044】

##### (5) フィルタリング処理

次に、本実施の形態1によるフィルタリングの処理手順について説明する。図3は、本実施の形態1によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置20におけるリクエストフィルタ30の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する（ステップS301）。

#### 【0045】

そして、リクエストフィルタ30の見積部32は、不正リクエストDB33に格納された不正アクセスのパターンおよび所定の見積ルール32aに基づいてHTTPリクエストの正当性を見積もる（ステップS302）。具体的には、HTTPリクエストが不正アクセスのパターンのいずれかに該当する場合には、不正リクエストである旨を見積もり、一方、HTTPリクエストが不正アクセスのパターンのいずれにも該当しない場合には、正当リクエストである旨を見積もる。

#### 【0046】

その後、リクエストフィルタ30の判定部34は、見積部32から受け取った見積結果および所定の判定ルール34aに基づいてHTTPリクエストをWebサーバ40に受け渡すか否かを判定する（ステップS303）。具体的には、見積部32により正当なリクエストである旨が見積もられたか否かを判定する。

#### 【0047】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップS303肯定）、リクエストフィルタ30の送信部35は、HTTPリクエストをプロセス間通信によりWebサーバ40に受け渡し（ステップS304）、Webサーバ40は、HTTPリクエストに応じた情報をクライアント装置10に送信するなどの正当判定時の処理をおこなう（ステップS305）。

#### 【0048】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップS303否定）、リクエストフィルタ30の送信部35は、HTTPリクエストのWebサーバ40への受け渡しを拒絶し（ステップS306）、リクエストフィルタ30の各部は、不正リクエストの破棄、格納媒体36

bへの格納、外部装置50への通報などの不正判定時の処理をおこなう（ステップS307）。

#### 【0049】

上述してきたように、本実施の形態1によれば、アクセス要求の送信元情報ではなく、アクセス要求の具体的な要求内容が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができる。これにより、不正クライアントと認定されていないクライアント装置10からの不正アクセスに対しても迅速かつ確実にWebサーバ40を防御することができる。

#### 【0050】

##### （実施の形態2）

ところで、上記実施の形態1では、クライアント装置からのHTTPリクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、HTTPリクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合についても同様に適用することができる。

#### 【0051】

そこで、本実施の形態2では、HTTPリクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合について説明する。なお、本実施の形態2においては、サーバクライアントシステムのシステム構成は図1に示すものと同様のものとなるので、ここではその詳細な説明を省略する。

#### 【0052】

まず最初に、本実施の形態2の特徴部分である見積部32および判定部34について説明する。本実施の形態2における見積部32は、クライアント装置10からのHTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、その見積値を判定部34に出力する。

#### 【0053】

具体的には、不正アクセスのパターンから一致するパターンの個数を算出することや、各パターンに危険度数を付与して一致するパターンの危険度数を算出することなどにより、HTTPリクエストの危険度を示すDI (Danger Index)と呼ばれる見積値を算出する。なお、見積値DIは、例えば1～100の範囲で整数値をとり、危険度が高いHTTPリクエストほど大きな値が算出されるというものである。

## 【0054】

本実施の形態2における判定部34は、見積部32により算出された見積値DIと所定の閾値とを比較してHTTPリクエストをWebサーバ40に受け渡すか否かを判定し、この判定結果を送信部35に出力する。

## 【0055】

具体的には、所定の閾値を50と仮定すると、見積部32からDIが50以上である見積値を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡さないものと判定し（不可判定）、一方、見積部32からDIが50未満である見積値を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡すものと判定する（可判定）。

## 【0056】

次に、本実施の形態2によるフィルタリングの処理手順について説明する。図4は、本実施の形態2によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置20におけるリクエストフィルタ30の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する（ステップS401）。

## 【0057】

そして、リクエストフィルタ30の見積部32は、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンに該当する度合に応じて見積値DIを算出する（ステップS402）。リクエストフィルタ30の判定部34は、見積部32により算出された見積値DIと所定の閾値とを比較してHTTPリクエストをWebサーバ40に受け渡すか否かを判定する（ステップS403）。具体的には、見積値DIが所定の閾値以上であるか否かを判定する。

## 【0058】

この判定により、見積値D I が所定の閾値未満であると判定された場合には（ステップS 4 0 3 肯定）、リクエストフィルタ3 0 の送信部3 5 は、H T T P リクエストをプロセス間通信によりW e b サーバ4 0 に受け渡し（ステップS 4 0 4 ）、W e b サーバ4 0 は、H T T P リクエストに応じた情報をクライアント装置1 0 に送信するなどの正当判定時の処理をおこなう（ステップS 4 0 5 ）。

## 【0059】

これとは反対に、見積値D I が所定の閾値以上であると判定された場合には（ステップS 4 0 3 否定）、リクエストフィルタ3 0 の送信部3 5 は、H T T P リクエストのW e b サーバ4 0 への受け渡しを拒絶し（ステップS 4 0 6 ）、リクエストフィルタ3 0 の各部は、不正リクエストの破棄、格納媒体3 6 b への格納、外部装置5 0 への通報などの不正判定時の処理をおこなう（ステップS 4 0 7 ）。

## 【0060】

上述してきたように、本実施の形態2によれば、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができる。これにより、不正クライアントと認定されていないクライアント装置1 0 からの不正アクセスに対してもある程度の幅を持ってW e b サーバ4 0 を防御することができる。

## 【0061】

## (実施の形態3)

ところで、上記実施の形態1 および2では、クライアント装置からの全てのH T T P リクエストについて不正アクセスのパターンに基づく見積もりをおこなう場合について説明したが、本発明にはこれに限定されるものではなく、一部のH T T P リクエストについてのみ見積もりをおこなう場合についても同様に適用することができる。

## 【0062】

そこで、本実施の形態3では、二階層からなるフィルタリング処理をおこない、一部のH T T P リクエストについてのみ不正アクセスのパターンに基づく見積

もりをおこなう場合について説明する。

#### 【0063】

図5は、本実施の形態3に係るサーバクライアントシステムの構成を示すブロック図である。なお、図1に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態3の特徴部分である事前判定部71および正当リクエストDB72について説明する。

#### 【0064】

サーバ装置60におけるリクエストフィルタ70の事前判定部71は、見積部32による正当性の見積もりの前に、正当リクエストDB72に格納された正当アクセスのパターンおよび所定の事前判定ルール71aに基づいてHTTPリクエストの見積もりを省くことができるか否かを判定する処理部である。

#### 【0065】

ここで、事前判定部71が判定に際して参照する正当リクエストDB72について説明すると、この正当リクエストDB72は、Webサーバ40に対する正当アクセスのパターンを格納したデータベースであり、具体的には、Webサーバ40上に存在するファイルのうちでリモートユーザに見られても構わないファイルのパスを記憶する。

#### 【0066】

このリモートユーザに見られても構わないファイルとは、パスワードファイルなどのリモートユーザが見るべきでないファイル以外のファイルであって、例えば、Webサーバ40に対するHTTPリクエストのリクエスト内容として非常に高い割合を有する画像ファイルなど、不正アクセスの可能性がほとんどないようなファイルが含まれる。

#### 【0067】

このような正当リクエストDB72を参照することにより、事前判定部71は、所定の事前判定ルール71aに基づいてHTTPリクエストの見積もりを省くことができるか否かを判定する。具体的には、HTTPリクエストが正当リクエストDB72に格納された正当アクセスのパターンのいずれかに該当する場合には、該HTTPリクエストの見積もりを省くことができるものと判定し、一方、

H T T P リクエストが正当リクエストDB72に格納された正当アクセスのパターンのいずれにも該当しない場合には、該H T T P リクエストの見積もりを省くことができないものと判定する。

## 【0068】

そして、事前判定部71は、見積もりを省くことができないものと判定されたH T T P リクエストのみを見積部32に出力し、見積もりを省くことができるものと判定されたH T T P リクエストについては、見積部32および判定部34による処理を省いて、送信部35を介してW e b サーバ40に受け渡す。

## 【0069】

なお、正当リクエストDB72に格納される正当アクセスのパターンは、W e b サーバ40に新たな画像ファイルが追加された場合などに応じて、更新部39により更新される。

## 【0070】

次に、本実施の形態3によるフィルタリングの処理手順について説明する。図6は、本実施の形態3によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置60におけるリクエストフィルタ70の受信部31は、クライアント装置10からのH T T P リクエストをW e b サーバ40が受信する前に受信する（ステップS601）。

## 【0071】

そして、リクエストフィルタ70の事前判定部71は、正当リクエストDB72に格納された正当アクセスのパターンおよび所定の事前判定ルール71aに基づいてH T T P リクエストの見積もりを省くことができるか否かを判定する（ステップS602）。具体的には、H T T P リクエストが正当リクエストDB72に格納された正当アクセスのパターンのいずれかに該当するか否かを判定する。

## 【0072】

この判定により、正当アクセスのパターンのいずれかに該当するものと判定された場合には（ステップS602肯定）、このH T T P リクエストの正当性の見積もりを省き、リクエストフィルタ70の送信部35は、H T T P リクエストをプロセス間通信によりW e b サーバ40に受け渡し（ステップS605）、W e

bサーバ40は、HTTPリクエストに応じた情報をクライアント装置10に送信するなどの正当判定時の処理をおこなう（ステップS606）。

#### 【0073】

これとは反対に、正当アクセスのパターンのいずれにも該当しないものと判定された場合には（ステップS602否定）、このHTTPリクエストを見積部32に受け渡し、上記実施の形態1または2によるフィルタリング処理と同様の処理をおこなう（ステップS603～608）。

#### 【0074】

すなわち、リクエストフィルタ70の見積部32は、HTTPリクエストの正当性を見積もり（ステップS603）、判定部34は、HTTPリクエストをWebサーバ40に受け渡すか否かを判定する（ステップS604）。

#### 【0075】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップS604肯定）、リクエストフィルタ70の送信部35は、HTTPリクエストをプロセス間通信によりWebサーバ40に受け渡し（ステップS605）、Webサーバ40は、HTTPリクエストに応じた情報をクライアント装置10に送信するなどの正当判定時の処理をおこなう（ステップS606）。

#### 【0076】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップS604否定）、リクエストフィルタ70の送信部35は、HTTPリクエストのWebサーバ40への受け渡しを拒絶し（ステップS607）、リクエストフィルタ70の各部は、不正リクエストの破棄、格納媒体36bへの格納、外部装置50への通報などの不正判定時の処理をおこなう（ステップS608）。

#### 【0077】

上述してきたように、本実施の形態3によれば、画像ファイルを要求するHTTPリクエストのような要求の割合は高いが攻撃性は極めて低いものについては、見積部32および判定部34による処理を省いて迅速な処理をおこなうことが

できるとともに、パスワードファイルやWebサーバ40上に存在しないファイルを要求するHTTPリクエストのような攻撃性が高いものについては、見積部32および判定部34による処理をおこなって、かかる攻撃を有効に防御することができる。

## 【0078】

なお、本実施の形態1～3では、クライアント装置10からのHTTPリクエストをフィルタリングする場合について説明したが、本発明はこれに限定されるものではなく、FTP(File Transfer Protocol)、telnet、コンソールなど、クライアント装置10からWebサーバ40に入力されるあらゆる情報をフィルタリングする場合に同様に適用することができる。

## 【0079】

また、本実施の形態1～3では、フィルタリング装置としてのリクエストフィルタ30、70をサーバ装置20、60に設けた場合について説明したが、本発明はこれに限定されるものではなく、例えば、それぞれのクライアント装置側にリクエストフィルタを設けたり、一つのリクエストフィルタにより複数のWebサーバを防御するなど、クライアント装置とWebサーバとの間にリクエストフィルタが介在するあらゆるシステム構成において同様に適用することができる。

## 【0080】

なお、本実施の形態1～3で説明したフィルタリング方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク(FD)、CD-ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

## 【0081】

## (実施の形態4)

ところで、上記実施の形態1～3では、サーバに対する不正アクセスのパターンを格納した不正リクエストDB33を参照することによって、アクセス要求の

要求内容から不正アクセスと把握できるアクセス要求を破棄する場合を説明したが、本発明はこれに限定されるものではなく、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求を破棄する場合についても同様に適用することができる。

#### 【0082】

すなわち、サーバに対する不正アクセスとしては、アクセス要求の要求内容から不正アクセスと把握されるアクセス要求の他に、アクセス要求の要求内容からは正当アクセスと把握されるが、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるべきアクセス要求がある。例えば、特定のクライアント装置10からのアクセス要求を集中的に受信している場合や、特定の要求内容からなるアクセス要求を集中的に受信している場合には、個々の要求内容からは正当アクセスと把握されたとしても、アクセス要求の統計からはサーバダウンを狙ったものと考えられるので、不正アクセスとみなされるべきである。

#### 【0083】

そこで、本実施の形態4では、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納したデータベースをも参照して正当性を見積ることによって、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求を破棄するフィルタリング処理も実行することができるようになっている。以下、本実施の形態4に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態4によるフィルタリングの処理手順とを説明する。

#### 【0084】

##### (1) サーバ装置の構成

まず最初に、本実施の形態4に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図7は、本実施の形態4に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態4におけるサーバ装置80は、Webサーバ40と、リクエストフィルタ81とを備え、さらに、このリクエストフィルタ81は、受信部31と、第1見積部82と、不正リクエストDB83と、第1判定部84と、第2見積部85と、統計的不正

リクエストDB86と、第2判定部87と、送信部88とを備える。

#### 【0085】

このうち、Webサーバ40および受信部31は、図1に示した同一符号を付している各部と同様の機能を有する。また、第1見積部82、不正リクエストDB83および第1判定部84は、図1に示した見積部32、不正リクエストDB33および判定部34と同様の機能をそれぞれ有し、上記実施の形態1または2に示したフィルタリング処理と同様の処理、すなわち、HTTPリクエストの要求内容から不正リクエストと把握できるHTTPリクエストを破棄するフィルタリング処理（パターンに基づくフィルタリング処理）を実行するものである。

#### 【0086】

すなわち、不正リクエストDB83は、サーバに対する不正アクセスのパターンを格納したデータベースである。また、第1見積部82は、不正リクエストDB83に格納された不正アクセスのパターンおよび所定の見積ルール82aに基づいてHTTPリクエストの正当性を見積もり、その見積結果（正当リクエスト若しくは不正リクエストである旨の見積結果、または見積値DI）を第1判定部84に出力する。

#### 【0087】

さらに、第1判定部84は、第1見積部82から受け取った見積結果および所定の判定ルール84aに基づいてHTTPリクエストをWebサーバ40に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値DIが所定の閾値以下であるか否か）を判定し、この判定結果を送信部88に出力するか、またはHTTPリクエストを第2見積部85に出力する。

#### 【0088】

これらによって、HTTPリクエストの要求内容から不正リクエストと把握されたHTTPリクエスト（すなわち、不正リクエストである旨が見積もられたHTTPリクエスト、または見積値DIが所定の閾値以下でなかったHTTPリクエスト）については、HTTPリクエストをWebサーバ40に受け渡さないものと判定され、不可判定が送信部88に出力されることとなる。

#### 【0089】

一方、これらによって、H T T Pリクエストの要求内容から不正リクエストと把握されなかったH T T Pリクエスト（すなわち、正当リクエストである旨が見積もられたH T T Pリクエスト、または見積値D Iが所定の閾値以下であったH T T Pリクエスト）については、W e bサーバ4 0に対するH T T Pリクエストの統計からみて不正リクエストとみなされるH T T Pリクエストを破棄するフィルタリング処理（統計に基づくフィルタリング処理）を実行するために、第2見積部8 5に出力されることとなる。

#### 【0090】

第2見積部8 5は、統計的不正リクエストD B 8 6に格納された統計的情報および所定の見積ルール8 5 aに基づいてH T T Pリクエストの正当性を見積もり、その見積結果を第2判定部8 7に出力する処理部である。

#### 【0091】

ここで、上記の統計的不正リクエストD B 8 6は、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納したデータベースである。具体的には、W e bサーバ4 0に対してH T T Pリクエストを送信したクライアント装置1 0のうち、所定時間内のリクエスト数が所定数を超えたクライアント装置1 0の送信元情報（I Pアドレス）や、W e bサーバ4 0に対して送信されたH T T Pリクエストの要求内容のうち、所定時間内のリクエスト数が所定数を超えた要求内容を格納する。

#### 【0092】

このような送信元情報や要求内容を格納することとしたのは、特定のクライアント装置1 0からのH T T Pリクエストを短時間で集中的に受信しているような場合や、特定の要求内容のH T T Pリクエストを短時間で集中的に受信しているような場合には、サーバダウンを狙った不正リクエストとみなすことができるからである。

#### 【0093】

そして、第2見積部8 5は、このような情報を格納した統計的不正リクエストD B 8 6を参照することにより、所定の見積ルール8 5 aに基づいてH T T Pリクエストの正当性の見積もりをおこなう。具体的には、H T T Pリクエストの送

信元情報が統計的不正リクエストDB86に格納された送信元情報のいずれかに該当する場合、またはHTTPリクエストの要求内容が統計的不正リクエストDB86に格納された要求内容のいずれかに該当する場合には、該HTTPリクエストは不正リクエストである旨を見積もる。

## 【0094】

一方、HTTPリクエストの送信元情報が統計的不正リクエストDB86に格納された送信元情報のいずれにも該当しない場合、およびHTTPリクエストの要求内容が統計的不正リクエストDB86に格納された要求内容のいずれかにも該当しない場合には、第2見積部85は、該HTTPリクエストは正当リクエストである旨を見積もる。

## 【0095】

第2判定部87は、第2見積部85から受け取った見積結果および所定の判定ルール87aに基づいてHTTPリクエストをWebサーバ40に受け渡すか否かを判定し、この判定結果を送信部88に出力する処理部である。具体的には、第2見積部85から不正リクエストである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡さないものと判定する（不可判定）。一方、第2見積部85から正当リクエストである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡すものと判定する（可判定）。

## 【0096】

送信部88は、第1判定部84および／または第2判定部87から受け取った判定結果に基づいて、受信部31から受け取ったHTTPリクエストの送信を制御するアクセス要求受渡手段である。具体的には、第2判定部87から可判定を受け取った場合には、HTTPリクエストをプロセス間通信によりWebサーバ40に受け渡す。一方、第1判定部84または第2判定部87から不可判定を受け取った場合には、HTTPリクエストのWebサーバ40への受け渡しを拒絶して、この不正リクエストを破棄する。

## 【0097】

すなわち、送信部88は、第1判定部84および第2判定部87によりWeb

サーバ40に受け渡すものと判定されたHTTPリクエスト（すなわち、HTTPリクエストの要求内容から不正リクエストと把握されず、かつ、Webサーバ40に対するHTTPリクエストの統計からみて不正リクエストとみなされなかったHTTPリクエスト）のみを、正当なHTTPリクエストとしてWebサーバ40に受け渡す。

#### 【0098】

なお、図7には図示していないが、本実施の形態4のリクエストフィルタ81は、図1に示した実施の形態1のリクエストフィルタ30と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。すなわち、本実施の形態4のリクエストフィルタ81においては、実施の形態1のリクエストフィルタ30と同様、ログ管理部は、所定の格納ルールに基づいて、送信部88によりWebサーバ40に受け渡されなかったHTTPリクエストに係る情報を所定の格納媒体に格納して管理する。

#### 【0099】

また、外部通信部は、所定の通報ルールに基づいて、送信部88によりWebサーバ40に受け渡されなかったHTTPリクエストに係る情報を外部装置に通報する。さらに、外部情報取得部は、所定の取得ルールに基づいて、更新部による更新処理に用いられる情報を、外部装置やWebサーバ40などのリクエストフィルタ81の外部から能動的または受動的に取得する。

#### 【0100】

そして、更新部は、所定の更新ルールに基づいて、不正リクエストDB33、見積ルール32a、判定ルール34a、見積ルール85a、判定ルール87a、管理ルール、通報ルール、取得ルールまたは更新ルールに格納された情報を更新するとともに、所定の更新ルールおよびWebサーバ40に対するアクセス要求の統計に基づいて、統計的不正リクエストDB86に格納された情報も更新する。

#### 【0101】

##### (2) フィルタリング処理

次に、本実施の形態4によるフィルタリングの処理手順について説明する。図

8は、本実施の形態4によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置80におけるリクエストフィルタ81の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する（ステップS801）。

## 【0102】

続いて、リクエストフィルタ81は、このHTTPリクエストを第1見積部82に受け渡し、上記実施の形態1または2によるフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行する（ステップS802、S803、S808およびS809）。

## 【0103】

すなわち、第1見積部82は、不正リクエストDB83に格納されたサーバに対する不正アクセスのパターンに基づいて、HTTPリクエストの正当性を見積もり（ステップS802）、第1判定部84は、HTTPリクエストをWebサーバ40に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値DIが所定の閾値以下であるか否か）を判定する（ステップS803）。

## 【0104】

この判定により、HTTPリクエストをWebサーバ40に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値DIが所定の閾値以上である場合）には（ステップS803否定）、送信部88は、HTTPリクエストのWebサーバ40への受け渡しを拒絶する（ステップS808）。さらに、リクエストフィルタ81の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップS809）。

## 【0105】

これとは反対に、HTTPリクエストをWebサーバ40に受け渡すものと判定された場合（すなわち、正当リクエストである旨が見積もられた場合、または見積値DIが所定の閾値以下である場合）には（ステップS803肯定）、HTTPリクエストは、統計に基づくフィルタリング処理を実行するために、第2見

積部85に出力される。そして、第2見積部85は、統計的不正リクエストDB86に格納された統計的情報および所定の見積ルール85aに基づいてHTTPリクエストの正当性を見積もる（ステップS804）。

#### 【0106】

具体的には、第2見積部85は、HTTPリクエストの送信元情報が統計的不正リクエストDB86に格納された送信元情報のいずれかに該当する場合、またはHTTPリクエストの要求内容が統計的不正リクエストDB86に格納された要求内容のいずれかに該当する場合には、該HTTPリクエストは不正リクエストである旨を見積もる。一方、HTTPリクエストの送信元情報が統計的不正リクエストDB86に格納された送信元情報のいずれにも該当しない場合、およびHTTPリクエストの要求内容が統計的不正リクエストDB86に格納された要求内容のいずれかにも該当しない場合には、第2見積部85は、該HTTPリクエストは正当リクエストである旨を見積もる。

#### 【0107】

その後、第2判定部87は、第2見積部85から受け取った見積結果および所定の判定ルール87aに基づいてHTTPリクエストをWebサーバ40に受け渡すか否か、すなわち正当リクエストである旨が見積もられたか否かを判定する（ステップS805）。

#### 【0108】

この判定により、正当リクエストである旨が見積もられた場合には（ステップS805肯定）、送信部88は、HTTPリクエストをプロセス間通信によりWebサーバ40に受け渡し（ステップS806）、Webサーバ40は、HTTPリクエストに応じた情報をクライアント装置10に送信するなどの正当判定時の処理をおこなう（ステップS807）。

#### 【0109】

これとは反対に、不正リクエストである旨が見積もられた場合には（ステップS805否定）、送信部88は、HTTPリクエストのWebサーバ40への受け渡しを拒絶し（ステップS808）、リクエストフィルタ81の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処

理をおこなう（ステップS809）。

【0110】

上記した一連の処理によって、HTTPリクエストの要求内容から不正リクエストと把握されず、かつ、Webサーバ40に対するHTTPリクエストの統計からみて不正リクエストとみなされなかつたHTTPリクエストのみが、正当なHTTPリクエストとしてWebサーバ40に受け渡されることとなる。

【0111】

上述してきたように、本実施の形態4によれば、サーバに対する不正アクセスのパターンを格納した不正リクエストDB83を参照して正当性を見積もるとともに、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正リクエストDB86をも参照して正当性を見積もることとしたので、アクセス要求の要求内容から不正アクセスと把握されるアクセス要求のみならず、サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求をも破棄することができる。これによって、クライアント装置10による不正アクセスからWebサーバ40を一層確実に防御することができる。

【0112】

（3）本実施の形態4の変形例

さて、これまで本実施の形態4について説明したが、本発明は上述した実施の形態4以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

【0113】

例えば、本実施の形態4では、統計的不正リクエストDB86が所定の送信元情報および要求内容を格納する場合を説明したが、本発明はこれに限定されるものではなく、統計的不正リクエストDB86が所定の送信元情報または要求内容のいずれか一方を格納する場合にも同様に適用することができる。

【0114】

すなわち、統計的不正リクエストDB86が所定の送信元情報のみを記憶する場合には、第2見積部85は、HTTPリクエストの送信元情報が統計的不正リ

クエストDB86に格納された送信元情報のいずれかに該当することを条件に該アクセス要求は不正アクセスである旨を見積もるとともに、いずれにも該当しないことを条件に該アクセス要求は正当アクセスである旨を見積もることとなる。

#### 【0115】

一方、統計的不正リクエストDB86が所定の要求内容のみを記憶する場合には、第2見積部85は、HTTPリクエストの要求内容が統計的不正リクエストDB86に格納された要求内容のいずれかに該当することを条件に該アクセス要求は不正アクセスである旨を見積もるとともに、いずれにも該当しないことを条件に該アクセス要求は正当アクセスである旨を見積もることとなる。

#### 【0116】

また、本実施の形態4では、HTTPリクエストの送信元情報や要求内容が、統計的不正リクエストDB86に格納された所定の送信元情報や要求内容に該当するか否かによって不正アクセスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、統計的不正リクエストDB86に格納された所定の送信元情報や要求内容に該当する度合に応じて不正アクセスであるか否かを判定する場合にも同様に適用することができる。

#### 【0117】

すなわち、この場合には、上記実施の形態2と同様、統計的不正リクエストDB86に格納された所定の送信元情報や要求内容にそれぞれ危険度数を付与しておき、第2見積部85は、HTTPリクエストの送信元情報や要求内容に対応する危険度数を用いて、HTTPリクエストの危険度を示すDI(Danger Index)と呼ばれる見積値を算出し、第2判定部87は、この算出された見積値DIと所定の閾値とを比較して不正アクセスであるか否かを判定することとなる。

#### 【0118】

また、本実施の形態4では、第2見積部85が、第1判定部84によりWebサーバ40に受け渡すものと判定されたHTTPリクエストのみについて正当性を見積もる場合、すなわち、パターンに基づくフィルタリング処理を実行した後に、統計に基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではない。

## 【0119】

例えば、第1見積部82が、第2判定部87によりWebサーバ40に受け渡すものと判定されたHTTPリクエストのみについて正当性を見積もる場合にも同様に適用することができる。この場合には、統計に基づくフィルタリング処理を実行した後に、パターンに基づくフィルタリング処理を実行することとなる。

## 【0120】

また、例えば、上記実施の形態3で説明した事前判定処理を追加し、事前判定部が、第2判定部87によりWebサーバ40に受け渡すものと判定されたアクセス要求のみについて事前判定処理をおこなう場合にも同様に適用することができる。この場合には、統計に基づくフィルタリング処理を実行した後に、事前判定処理がおこなわれ、この事前判定処理に続いて、パターンに基づくフィルタリング処理を実行することとなる。

## 【0121】

なお、事前判定処理を追加する場合には、統計に基づくフィルタリング処理よりも後に事前判定処理をおこなう必要がある。この統計に基づくフィルタリング処理よりも前に事前判定処理をおこなうと、上記のようなHTTPリクエストが正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するものと判定されてしまい、統計に基づくフィルタリング処理によって破棄されることなく、Webサーバ40に受け渡されるおそれが生じるからである。

## 【0122】

さらに、本発明は、パターンに基づくフィルタリング処理や統計に基づくフィルタリング処理を階層的に実行する場合に限定されず、これらの各処理を並列的に実行する場合にも同様に適用することができる。すなわち、この場合には、図9に示すように、サーバ装置90のリクエストフィルタ91は、受信部31と送信部88との間に、パターンに基づくフィルタリング処理を実行する第1見積部82および第1判定部84と、統計に基づくフィルタリング処理を実行する第2見積部85および第2判定部87とを、並列的に備えることとなる。このようなリクエストフィルタ91を構成することにより、不正アクセスであるか否かを一層迅速に判定することが可能になる。

## 【0123】

(実施の形態5)

ところで、上記実施の形態4では、統計的不正リクエストDB86を参照して統計に基づくフィルタリング処理を実行する場合を説明したが、本発明は、この統計的不正リクエストDB86に格納された情報を動的に更新しながら、フィルタリング処理を実行することもできる。

## 【0124】

すなわち、実施の形態4では、第2見積部85は、HTTPリクエストの送信元情報が統計的不正リクエストDB86に格納された送信元情報のいずれかに該当する場合、またはHTTPリクエストの要求内容が統計的不正リクエストDB86に格納された要求内容のいずれかに該当する場合には、該HTTPリクエストは不正リクエストである旨を見積もることとしている。

## 【0125】

しかしながら、特定のクライアント装置10（送信元情報）からのHTTPリクエストや特定の要求内容のHTTPリクエストの受信が急激に増加しているような状況において、この特定の送信元情報や要求内容が統計的不正リクエストDB86にリアルタイムで追加されなかったのでは、サーバに対するHTTPリクエストの統計からみて不正リクエストとみなされるHTTPリクエストがWebサーバ40に送信されてしまう。

## 【0126】

その一方で、統計的不正リクエストDB86に格納された特定の送信元情報や要求内容のHTTPリクエストの受信が減少しているような状況において、この特定の送信元情報や要求内容が統計的不正リクエストDB86からリアルタイムで削除されなかったのでは、サーバに対するHTTPリクエストの統計からみて不正リクエストとはみなされないHTTPリクエストまでが破棄されてしまう。

## 【0127】

そこで、本実施の形態5では、統計的不正リクエストDB86に格納された情報を動的に更新することによって、サーバに対するHTTPリクエストの統計からみて不正リクエストとみなされるHTTPリクエストを精度良く確実に破棄す

することができるようしている。以下、本実施の形態5に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。

#### 【0128】

図10は、本実施の形態5に係るサーバクライアントシステムの構成を示すブロック図である。なお、図1または図7に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態5の特徴部分であるアクセス管理部102および動的更新部103について説明する。

#### 【0129】

サーバ装置100におけるリクエストフィルタ101のアクセス管理部102は、サーバ装置100に対して送信されたH T T Pリクエストの送信元情報、要求内容および送信時刻を履歴として管理するメモリである。

#### 【0130】

そして、動的更新部103は、アクセス管理部102により管理される情報および所定の更新ルール103aに基づいて、統計的不正リクエストDB86に格納された情報を動的に更新する処理部である。具体的には、アクセス管理部102を参照し、特定のクライアント装置10からW e bサーバ40に対して送信された所定時間内のH T T Pリクエスト数が所定の上限数を超えた場合には、この送信元情報を統計的不正リクエストDB86に追加する。

#### 【0131】

その一方で、動的更新部103は、統計的不正リクエストDB86に格納された送信元情報のクライアント装置10からW e bサーバ40に対して送信された所定時間内のH T T Pリクエスト数が所定の下限数を下回った場合には、この送信元情報を統計的不正リクエストDB86から削除する。

#### 【0132】

さらに、動的更新部103は、アクセス管理部102を参照し、W e bサーバ40に対して送信された特定のH T T Pリクエストのリクエスト数が所定時間内に所定の上限数を超えた場合には、このH T T Pリクエストの要求内容を統計的不正リクエストDB86に追加する一方、統計的不正リクエストDB86に格納された要求内容のH T T Pリクエストのリクエスト数が所定時間内に所定の下限

数を下回った場合には、この要求内容を統計的不正リクエストDB86から削除する。

【0133】

なお、上記した「所定の上限数」は、これを超えた場合にはサーバダウンを狙った不正アクセスとみなれるべきという閾値であり、一方、上記した「所定の下限数」は、これを下回った場合にはサーバダウンを狙った不正アクセスとみなれるべきでないという閾値である。そして、これらの上限数および下限数は、Webサーバ40の処理能力などを考慮して設定される。

【0134】

上述してきたように、本実施の形態5によれば、所定時間内にWebサーバ40に対してHTTPリクエストを送信した各クライアント装置10ごとのリクエスト数や、所定時間内にWebサーバ40に対して送信されたHTTPリクエストの各要求内容ごとのリクエスト数に応じて、統計的不正リクエストDB86に格納される送信元情報や要求内容を追加したり削除することとしたので、Webサーバ40に対するHTTPリクエストの統計からみて不正リクエストとみなされるHTTPリクエストを精度良く確実に破棄することができる。

【0135】

なお、本実施の形態5では、統計的不正リクエストDB86に格納される送信元情報および要求内容とともに更新する場合を説明したが、本発明はこれに限定されるものではなく、統計的不正リクエストDB86に送信元情報または要求内容のいずれか一方を格納する場合には、格納される送信元情報または要求内容のみを追加したり削除するなど、統計的不正リクエストDB86に格納される情報に応じて更新することができる。

【0136】

また、本実施の形態5では、アクセス管理部102のみを参照して、統計的不正リクエストDB86を動的に更新する場合を説明したが、本発明はこれに限定されるものではなく、例えば、ログ管理部36およびアクセス管理部102の両者を参照して、統計的不正リクエストDB86を動的に更新する場合にも同様に適用することができる。

## 【0137】

すなわち、ログ管理部36に追加された送信元情報を統計的不正リクエストDB86にも追加したり、また、ログ管理部36に格納されている送信元情報については、統計的不正リクエストDB86において高度の危険度数を付与したり、さらに、リクエスト数が所定の下限値を下回った場合でも、統計的不正リクエストDB86から削除しないなど、ログ管理部36をも参照して統計的不正リクエストDB86を動的に更新することができる。

## 【0138】

## (実施の形態6)

ところで、上記実施の形態1～5では、クライアント装置10から送信されたHTTPリクエストに対して種々の見積もりをおこなって不正アクセスを破棄する場合を説明したが、本発明はこれに限定されるものではなく、HTTPリクエストに応じてWebサーバ40からクライアント装置10に送信されるレスポンスに対しても、その正当性を見積もって不正なレスポンスを破棄することもできる。

## 【0139】

すなわち、上記実施の形態1～5では、不正リクエストのパターンを不正リクエストDB33などに格納し、クライアント装置10からのHTTPリクエストが不正リクエストのパターンに一致するか否かなどによって不正アクセスであるか否かを判定したが、不正リクエストのなかには、パターンとして記述し難い不正リクエストもある。例えば、Webサーバ40が所有しないファイルを要求するHTTPリクエストを送信することによって、ディレクトリ情報など、Webサーバ40の外部に漏れてはいけない秘匿情報をレスポンスとして受信しようとする不正アクセスなどである。

## 【0140】

このような不正アクセスは、Webサーバ40が所有しないファイルを要求するものであるところ、パターンとして記述し難いため、不正リクエストのパターンに一致するか否かなどを見積もるだけでは、これを不正アクセスと判定することができない。一方、このような不正アクセスに応じてWebサーバ40からク

ライアント装置10に送信されるレスポンスには、ディレクトリ情報など、Webサーバ40の外部に漏れてはいけない秘匿情報が含まれるので、このような秘匿情報がレスポンスに含まれるか否かを見積もれば、パターンとして記述し難い不正アクセスに対しても対応することができると考えられる。

#### 【0141】

そこで、本実施の形態6では、クライアント装置10に対して送信されるべきでない不正レスポンスのパターンを格納したデータベースを参照して、レスポンスの正当性を見積もることによって、パターンとして記述し難い不正アクセスに応じてクライアント装置10に送信されようとする不正なレスポンスをも破棄することができるようしている。以下、本実施の形態6に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態6によるフィルタリングの処理手順とを説明する。

#### 【0142】

##### (1) サーバ装置の構成

まず最初に、本実施の形態6に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図11は、本実施の形態6に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態6におけるサーバ装置110は、Webサーバ40と、リクエストフィルタ111とを備え、さらに、このリクエストフィルタ111は、受信部31と、見積部32と、不正リクエストDB33と、判定部34と、送信部35と、レスポンス受信部112と、レスポンス見積部113と、不正レスポンスDB114と、レスポンス判定部115と、レスポンス送信部116とを備える。

#### 【0143】

このうち、受信部31、見積部32、不正リクエストDB33、判定部34および送信部35は、図1に示した同一符号を付している各部と同様の機能を有し、上記実施の形態1または2に示したフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行するものである。

#### 【0144】

ところで、Webサーバ40が所有しないファイルを要求するHTTPリクエ

ストなど、不正アクセスのパターンとして記述することが困難なH T T Pリクエストについては、不正リクエストDB33にはパターンとして格納されないので、不正リクエストとして破棄されることなく、W e bサーバ40に送信されることとなる。しかしながら、かかる不正リクエストに応じてW e bサーバ40からクライアント装置10に送信されようとするレスポンスは、以下に説明する各部の処理によって、不正なレスポンスとして破棄される。

#### 【0145】

レスポンス受信部112は、W e bサーバ40からのレスポンスをクライアント装置10に送信する前に受信する処理部である。なお、レスポンス受信部112によりW e bサーバ40から受信したレスポンスは、レスポンス見積部113およびレスポンス送信部116に出力される。

#### 【0146】

レスポンス見積部113は、不正レスポンスDB114に格納された不正レスポンスのパターンおよび所定の見積ルール113aに基づいてレスポンスの正当性を見積もり、その見積結果をレスポンス判定部115に出力する処理部である。

#### 【0147】

ここで、上記の不正レスポンスDB114は、H T T Pリクエストに応じてW e bサーバ40からクライアント装置10に対してサービスとして送信されるレスポンスのうち、クライアント装置10に対して送信されるべきでない不正レスポンスのパターンを格納したデータベースである。具体的には、ディレクトリ情報など、W e bサーバ40の外部に漏れてはいけない秘匿情報をパターンとして記憶する。

#### 【0148】

これらの秘匿情報をパターンとして記憶することとしたのは、W e bサーバ40が所有しないファイルを要求するH T T Pリクエストに対するレスポンスとして、これらの秘匿情報がクライアント装置10に送信されるおそれがあるからである。

#### 【0149】

そして、レスポンス見積部113は、このような秘匿情報を格納した不正レスポンスDB114を参照することにより、所定の見積ルール113aに基づいてレスポンスの正当性の見積もりをおこなう。具体的には、レスポンスが不正レスポンスDB114に格納された秘匿情報パターンのいずれかに該当する場合には、該レスポンスは不正レスポンスである旨を見積もり、一方、レスポンスが不正レスポンスDB114に格納された秘匿情報パターンのいずれにも該当しない場合には、該レスポンスは正当レスポンスである旨を見積もる。

## 【0150】

レスポンス判定部115は、レスポンス見積部113から受け取った見積結果および所定の判定ルール115aに基づいてレスポンスをクライアント装置10に送信するか否かを判定し、この判定結果をレスポンス送信部116に出力する処理部である。具体的には、レスポンス見積部113から不正レスポンスである旨の見積結果を受け取った場合には、レスポンスをクライアント装置10に送信しないものと判定し（不可判定）、一方、レスポンス見積部113から正当レスポンスである旨の見積結果を受け取った場合には、レスポンスをクライアント装置10に送信するものと判定する（可判定）。

## 【0151】

レスポンス送信部116は、レスポンス判定部115から受け取った判定結果に基づいて、レスポンス受信部112から受け取ったレスポンスの送信を制御する処理部である。具体的には、レスポンス判定部115から可判定を受け取った場合には、レスポンスをネットワーク1を介してクライアント装置10に送信する。一方、レスポンス判定部115から不可判定を受け取った場合には、レスポンスのクライアント装置10への送信を拒絶して、このレスポンスを不正レスポンスとして破棄する。

## 【0152】

なお、図7には図示していないが、本実施の形態6のリクエストフィルタ111は、図1に示した実施の形態1のリクエストフィルタ30と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。すなわち、本実施の形態6のリクエストフィルタ111においては、実施の形態1のリクエス

トフィルタ30と同様、ログ管理部は、所定の格納ルールに基づいて、レスポンス送信部116によりクライアント装置10に送信されなかったレスポンスに係る情報や、このレスポンスの起因となったHTTPリクエストに係る情報を所定の格納媒体に格納して管理する。

#### 【0153】

また、外部通信部は、所定の通報ルールに基づいて、レスポンス送信部116によりクライアント装置10に送信されなかったレスポンスに係る情報や、このレスポンスの起因となったHTTPリクエストに係る情報を外部装置に通報する。さらに、外部情報取得部は、所定の取得ルールに基づいて、更新部による更新処理に用いられる情報を、外部装置やWebサーバ40などのリクエストフィルタ111の外部から能動的または受動的に取得する。

#### 【0154】

そして、更新部は、所定の更新ルールに基づいて、不正レスポンスDB114、見積ルール113a、判定ルール115a、管理ルール、通報ルール、取得ルールまたは更新ルールに格納された情報を更新する。例えば、外部情報取得部から新たな不正レスポンスのパターンを受け付けた場合には、この不正レスポンスのパターンを不正レスポンスDB114に格納し、また見積ルール113aの変更指示情報を受け付けた場合には、この変更指示情報に応じて見積ルール113aを変更する。

#### 【0155】

##### (2) フィルタリング処理

次に、本実施の形態6によるフィルタリングの処理手順について説明する。図12は、本実施の形態6によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置110におけるリクエストフィルタ111の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する(ステップS1201)。

#### 【0156】

続いて、リクエストフィルタ111は、このHTTPリクエストを見積部32に受け渡し、上記実施の形態1または2によるフィルタリング処理と同様の処理

、すなわち、パターンに基づくフィルタリング処理を実行する（ステップS1202～S1205、ステップS1210およびS1211）。

#### 【0157】

すなわち、見積部32は、不正リクエストDB33に格納されたサーバに対する不正アクセスのパターンに基づいて、HTTPリクエストの正当性を見積もり（ステップS1202）、判定部34は、HTTPリクエストをWebサーバ40に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値DIが所定の閾値以下であるか否か）を判定する（ステップS1203）。

#### 【0158】

この判定により、HTTPリクエストをWebサーバ40に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値DIが所定の閾値以上である場合）には（ステップS1203否定）、送信部35は、HTTPリクエストのWebサーバ40への受け渡しを拒絶する（ステップS1210）。さらに、リクエストフィルタ111の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップS1211）。

#### 【0159】

これとは反対に、正当リクエストである旨が見積もられた場合には（ステップS1203肯定）、送信部35は、HTTPリクエストをプロセス間通信によりWebサーバ40に送信し（ステップS1204）、Webサーバ40は、HTTPリクエストに応じたレスポンスを作成するなど、正当判定時の処理をおこなう（ステップS1205）。

#### 【0160】

続いて、リクエストフィルタ111のレスポンス受信部112は、Webサーバ40からレスポンスを受信する（ステップS1206）。そして、レスポンス見積部113は、不正レスポンスDB114に格納された秘匿情報パターンおよび所定の見積ルール113aに基づいてレスポンスの正当性を見積もる（ステップS1207）。具体的には、レスポンスが不正レスポンスDB114に格納さ

れた秘匿情報パターンのいずれかに該当する場合には、該レスポンスは不正レスポンスである旨を見積もり、一方、レスポンスが不正レスポンスDB114に格納された秘匿情報パターンのいずれにも該当しない場合には、該レスポンスは正当レスポンスである旨を見積もる。

## 【0161】

その後、レスポンス判定部115は、レスポンス見積部113から受け取った見積結果および所定の判定ルール115aに基づいて、レスポンスをクライアント装置10に送信するか否かを判定する（ステップS1208）。具体的には、正当なレスポンスとして見積もられたか否かを判定する。

## 【0162】

この判定により、正当なレスポンスである旨が見積もられたものと判定された場合には（ステップS1208肯定）、レスポンス送信部116は、レスポンスをネットワーク1を介してクライアント装置10に送信する（ステップS1209）。

## 【0163】

これとは反対に、不正なレスポンスである旨が見積もられたものと判定された場合には（ステップS1208否定）、レスポンス送信部116は、レスポンスのクライアント装置10への送信を拒絶し（ステップS1212）、リクエストフィルタ111の各部は、不正レスポンスの破棄、格納媒体への格納、外部装置への通報など、不正判定時の処理をおこなう（ステップS1213）。

## 【0164】

上記した一連の処理によって、正当なアクセスに応じた正当なレスポンス、すなわち不正アクセスとして破棄されず、かつ、不正レスポンスとして破棄されなかったレスポンスのみが、クライアント装置10に送信されることとなる。

## 【0165】

上述してきたように、本実施の形態6によれば、クライアント装置10から送信されたHTTPリクエストに対して種々の見積もりをおこなって不正アクセスを破棄するとともに、HTTPリクエストに応じてWebサーバ40からクライアント装置10に送信されるレスポンスに対しても、その正当性を見積もって不

正なレスポンスを破棄することとしたので、不正アクセスのパターンとして記述される不正アクセスのみならず、不正アクセスのパターンとして記述し難い不正アクセスに応じた不正なレスポンスをも破棄することができる。これによって、クライアント装置10による不正アクセスからWebサーバ40を一層確実に防御することができる。

## 【0166】

## (3) 本実施の形態6の変形例

さて、これまで本実施の形態6について説明したが、本発明は上述した実施の形態6以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

## 【0167】

例えば、本実施の形態6では、Webサーバ40からのレスポンスが不正レスポンスDB114に格納された不正レスポンスのパターンに該当するか否かによって不正レスポンスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、不正レスポンスDB114に格納された不正レスポンスのパターンに該当する度合に応じて不正レスポンスであるか否かを判定する場合にも同様に適用することができる。

## 【0168】

すなわち、この場合には、上記実施の形態2と同様、レスポンス見積部113は、不正レスポンスDB114に格納された不正レスポンスのパターンから一致するパターンの個数を算出することや、各パターンに危険度数を付与して一致するパターンの危険度数を算出することなどにより、レスポンスの危険度を示すDI(Danger Index)と呼ばれる見積値を算出し、レスポンス判定部115は、この算出された見積値と所定の閾値とを比較してレスポンスをクライアント装置10に送信するか否かを判定することとなる。

## 【0169】

また、本実施の形態6では、クライアント装置10から送信されたHTTPリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態3で説明し

た事前判定処理や、上記実施の形態4で説明した統計に基づくフィルタリング処理とともに実行する場合にも同様に適用することができる。

#### 【0170】

##### (実施の形態7)

ところで、上記実施の形態1～6では、暗号処理されていないHTTPリクエストや暗号処理されていないレスポンスに対してフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、暗号処理がなされたHTTPリクエストや暗号処理がなされたレスポンスに対してフィルタリング処理を実行する場合にも同様に適用することができる。

#### 【0171】

すなわち、上記実施の形態1～6では、Webサーバ40が、クライアント装置10から暗号処理されていないHTTPリクエストを受信するとともに、暗号処理されていないレスポンスをクライアント装置10に送信することを前提にしている。しかしながら、Webサーバ40によっては、提供するサービスの秘匿性などを確保するために、クライアント装置10から暗号処理がなされたHTTPリクエストを受信するとともに、暗号処理がなされてたレスポンスをクライアント装置10に送信するようにしたものもある。

#### 【0172】

このようなWebサーバ40に対して、上記実施の形態1～6で説明したフィルタリング処理を単純に適用したのでは、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスを破棄することはできない。このため、不正アクセスからWebサーバ40を防御することができず、さらに、Webサーバ40からクライアント装置10に不正レスポンスが送信されるおそれがある。

#### 【0173】

そこで、本実施の形態7では、暗号処理がなされたHTTPリクエストを復号するとともに、暗号処理がなされたレスポンスを復号することによって、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスをも破棄することができるようになっている。以下、本実施の形態7に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。

## 【0174】

図13は、本実施の形態7に係るサーバクライアントシステムの構成を示すブロック図である。なお、図1または図11に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態7の特徴部分である復号部122および復号部123について説明する。

## 【0175】

サーバ装置120におけるリクエストフィルタ121の復号部122は、所定の暗号処理がなされたHTTPリクエストを復号する復号手段である。具体的には、受信部31から暗号処理がなされたHTTPリクエストを受け取った後、このHTTPリクエストを復号し、復号したHTTPリクエストを見積部32に出力する。これによって、見積部32は、上記実施の形態1または2で説明した見積処理を実行することとなる。

## 【0176】

なお、受信部31は、暗号処理がなされたHTTPリクエストを送信部35に出力するので、Webサーバ40には、暗号処理がなされたHTTPリクエストが送信されることとなる。これによって、一つのリクエストフィルタ121により複数のWebサーバ40を防御するために、リクエストフィルタ121と複数のWebサーバ40とをインターネットなどの非専用回線で接続した場合でも、HTTPリクエストの秘匿性を確保することができる。

## 【0177】

一方、復号部123は、所定の暗号処理がなされたレスポンスを復号する第2の復号手段である。具体的には、レスポンス受信部112から暗号処理がなされたレスポンスを受け取った後、このレスポンスを復号し、復号したレスポンスをレスポンス見積部113に出力する。これによって、レスポンス見積部113は、上記実施の形態6で説明した見積処理を実行することとなる。

## 【0178】

なお、レスポンス受信部112は、暗号処理がなされたレスポンスをレスポンス送信部116に出力するので、クライアント装置10には、暗号処理がなされたレスポンスが送信されることとなる。これによって、クライアント装置10に

送信されるレスポンスの秘匿性を確保することができる。

【0179】

上述してきたように、本実施の形態7によれば、暗号処理がなされたHTTPリクエストを復号するとともに、暗号処理がなされたレスポンスを復号することとしたので、クライアント装置10から暗号処理がなされたHTTPリクエストを受信するとともに、暗号処理がなされてたレスポンスをクライアント装置10に送信するようにしたWebサーバ40に適用する場合においても、暗号化がなされた不正アクセスや暗号化がなされた不正レスポンスを破棄することができる。これによって、不正アクセスからWebサーバ40を確実に防御することができ、さらに、Webサーバ40からクライアント装置10に不正レスポンスが送信されるおそれを確実に排除することができる。

【0180】

なお、本実施の形態7では、HTTPリクエストおよびレスポンスを復号する場合を説明したが、本発明はこれに限定されるものではなく、HTTPリクエストのみを復号する場合や、レスポンスのみを復号する場合など、Webサーバ40の処理態様（暗号処理がなされたHTTPリクエストを受信するか否か、暗号処理がなされたレスポンスを送信するか否かなど）に応じて、HTTPリクエストまたはレスポンスの一方を復号する場合に同様に適用することができる。

【0181】

また、本実施の形態7では、リクエストフィルタ121によりHTTPリクエストを復号した後に、Webサーバ40には、暗号処理がなされたHTTPリクエストを送信する場合を説明したが、本発明はこれに限定されるものではなく、Webサーバ40に対して、復号されたHTTPリクエストを送信する場合にも同様に適用することができる。なお、この場合には、Webサーバ40の復号手段を省略することができる。

【0182】

また、本実施の形態7では、クライアント装置10から送信されたHTTPリクエストに対しては、パターンに基づくfiltrating処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態3で説明し

た事前判定処理や、上記実施の形態4で説明した統計に基づくフィルタリング処理をともに実行する場合にも同様に適用することができる。なお、この場合にも、事前判定処理や統計に基づくフィルタリング処理に先だって、本実施の形態7で説明した復号処理が実行される。

## 【0183】

## (実施の形態8)

ところで、上記実施の形態1～7では、不正なHTTPリクエストや不正なレスポンスを破棄する場合を説明したが、本発明はこれに限定されるものではなく、クライアント装置10に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することもできる。

## 【0184】

すなわち、不正なHTTPリクエストや不正なレスポンスを破棄するだけでは、不正アクセスを試行した攻撃者（クラッカー）は、不正アクセスが失敗したこと気にいて、新たな別の不正アクセスを試行するおそれがある。このため、望ましくは、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐことによって、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することが必要とされる。

## 【0185】

ところで、従来より、不正アクセスからサーバを保護する技術として、おとりシステム（おとりサーバ、ハニーポット）と呼ばれる技術が一般的に知られている。このおとりシステムは、セキュリティホールを有するといった脆弱なサーバを装って、攻撃者による不正アクセスの試行を全てロギングするものである。

## 【0186】

すなわち、攻撃者は一般的に、ネットワーク上のセキュリティレベルの低いサーバを攻撃対象とする行動志向を有するので、おとりシステムは、脆弱なサーバを装って、攻撃者がおとりシステムにアクセスしたならば、真のサーバ（不正アクセスから保護したいサーバ）であるかのようにログインバナーの返信などをする。そして、攻撃者が辞書を用いたパスワードクラッキングなどによってログインを試行してきた場合には、これらの行動を全てログとして安全に記録する。

## 【0187】

このようにして、おとりシステムは、真のサーバが攻撃されるまでの時間を稼ぎ、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口（攻撃に用いる辞書など）を解析する。そして、この攻撃手口の解析結果や時間稼ぎによって、真のサーバに対する防御策を講じることが可能になる。

## 【0188】

しかしながら、おとりシステムは、不正アクセスから保護したい真のサーバのおとりにはなれないという問題点がある。すなわち、あるサーバを保護しようとする場合、一般的に、おとりシステムは、そのサーバのミラーサーバ若しくはテストサーバを装って（それらを連想させる名前を付与されて）運用される。これは、真のサーバに対して正規にアクセスしようとする正規ユーザのために、真のサーバについては、真のサーバとわかる名前を付与して運用しなければならないからである。

## 【0189】

したがって、真のサーバを保護するために、おとりシステムを導入しても、攻撃者がおとりシステムに目もくれず、真のサーバを攻撃してきたような場合には、おとりシステムの機能は没却され、真のサーバを保護するという目的を達成することができなくなってしまう。

## 【0190】

そこで、本実施の形態8では、おとりシステムではなく、Webサーバ40に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを導入することによって、不正アクセスを試行したクライアント装置10に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することができるようになっている。以下、本実施の形態8に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態8によるフィルタリングの処理手順とを説明する。

## 【0191】

(1) サーバ装置の構成

まず最初に、本実施の形態8に係るサーバクライアントシステムにおけるサーバ装置の構成を説明する。図14は、本実施の形態8に係るサーバクライアントシステムの構成を示すブロック図である。同図に示すように、本実施の形態8におけるサーバ装置130は、Webサーバ40と、リクエストフィルタ131とを備え、さらに、このリクエストフィルタ131は、受信部31と、見積部32と、不正リクエストDB33と、判定部34と、送信部35と、偽レスポンス作成部132と、偽レスポンスDB133と、レスポンス送信部134とを備える。

#### 【0192】

このうち、受信部31、見積部32、不正リクエストDB33、判定部34および送信部35は、図1に示した同一符号を付している各部と同様の機能を有し、上記実施の形態1または2に示したフィルタリング処理と同様の処理、すなわち、パターンに基づくフィルタリング処理を実行するものである。このフィルタリング処理によって、不正なHTTPリクエストは、Webサーバ40に送信されることなく、偽レスポンス作成部132に出力される。

#### 【0193】

偽レスポンス作成部132は、偽レスポンスDB133および所定の作成ルールに基づいて、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストのパターンに対応した偽のレスポンスを作成する処理部である。

#### 【0194】

ここで、上記の偽レスポンスDB133は、Webサーバ40に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納したデータベースである。具体的には、不正リクエストDB33に格納された不正アクセスのパターンに対応付けて偽のレスポンスを記憶する。例えば、Webサーバ40上のパスワードファイルをリクエストする不正アクセスのパターンに対応付けられた、架空の情報からなる偽のパスワードファイルや、Webサーバ40に不正にログインしようとする不正アクセスのパターンに対応付けられた、偽のログインバナーなどを記憶する。

#### 【0195】

そして、偽レスポンス作成部132は、このような情報を格納した偽レスポンスDB133を参照することにより、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストのパターンに対応した偽のレスポンスを作成する。

#### 【0196】

具体的には、Webサーバ40上のパスワードファイルをリクエストするHTTPリクエストが、不正アクセスとして偽レスポンス作成部132に入力された場合には、偽レスポンスDB133に格納された偽のパスワードファイルを用いて偽のレスポンスを作成する。また、Webサーバ40に不正にログインしようとするHTTPリクエストが、不正アクセスとして偽レスポンス作成部132に入力された場合には、偽レスポンスDB133に格納された偽のログインバナーを用いて偽のレスポンスを作成する。

#### 【0197】

レスポンス送信部134は、Webサーバ40により正当に作成された正当レスポンスや、偽レスポンス作成部132により作成された偽のレスポンスをクライアント装置10に送信する処理部である。なお、図14には図示していないが、本実施の形態8のリクエストフィルタ131は、図1に示した実施の形態1のリクエストフィルタ30と同様、ログ管理部、外部通信部、外部情報取得部および更新部を備えるものである。

#### 【0198】

##### (2) フィルタリング処理

次に、本実施の形態8によるフィルタリングの処理手順について説明する。図15は、本実施の形態8によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置130におけるリクエストフィルタ131の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する(ステップS1501)。

#### 【0199】

続いて、リクエストフィルタ131は、このHTTPリクエストを見積部32に受け渡し、上記実施の形態1または2によるフィルタリング処理と同様の処理

、すなわち、パターンに基づくフィルタリング処理を実行する（ステップS1502～S1505、ステップS1507およびS1508）。

#### 【0200】

すなわち、見積部32は、不正リクエストDB33に格納されたサーバに対する不正アクセスのパターンに基づいて、HTTPリクエストの正当性を見積もり（ステップS1502）、判定部34は、HTTPリクエストをWebサーバ40に受け渡すか否か（すなわち、正当リクエストである旨が見積もられたか否か、または見積値DIが所定の閾値以下であるか否か）を判定する（ステップS1503）。

#### 【0201】

この判定により、正当リクエストである旨が見積もられた場合には（ステップS1503肯定）、送信部35は、HTTPリクエストをプロセス間通信によりWebサーバ40に送信し（ステップS1504）、Webサーバ40は、HTTPリクエストに応じたレスポンスを作成するなど、正当判定時の処理をおこなう（ステップS1505）。続いて、レスポンス送信部134は、Webサーバ40により作成されたレスポンスをクライアント装置10に送信する（ステップS1506）

#### 【0202】

これとは反対に、HTTPリクエストをWebサーバ40に受け渡さないものと判定された場合（すなわち、不正リクエストである旨が見積もられた場合、または見積値DIが所定の閾値以上である場合）には（ステップS1503否定）、送信部35は、HTTPリクエストのWebサーバ40への受け渡しを拒絶する（ステップS1507）。さらに、リクエストフィルタ131の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなう（ステップS1508）。

#### 【0203】

続いて、偽レスポンス作成部132は、偽レスポンスDB133および所定の作成ルール132aに基づいて、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストのパターンに対応した偽のレスポンスを作成す

る（ステップS1509）。具体的には、偽レスポンスDB133に格納された偽のパスワードファイルを用いた偽のレスポンスや、偽レスポンスDB133に格納された偽のログインバナーを用いた偽のレスポンスなどを作成する。その後、レスポンス送信部134は、偽レスポンス作成部132により作成された偽のレスポンスをクライアント装置10に送信する（ステップS1510）。

#### 【0204】

上記した一連の処理によって、不正アクセスのパターンに該当するHTTPリクエストをWebサーバ40に送信してきたクライアント装置10に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信されることとなる。

#### 【0205】

上述してきたように、本実施の形態8によれば、Webサーバ40に対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスDB133を導入することとしたので、不正アクセスを試行したクライアント装置10に対して、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信することができる。これによって、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐことができ、さらに、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することもできるので、クライアント装置10による不正アクセスからWebサーバ40を一層確実に防御することが可能になる。

#### 【0206】

なお、本実施の形態8では、クライアント装置10から送信されたHTTPリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態3で説明した事前判定処理や、上記実施の形態4で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態6で説明したレスポンスのフィルタリング処理とともに実行する場合にも同様に適用することができる。

#### 【0207】

すなわち、例えば、上記実施の形態6で説明したレスポンスのフィルタリング

処理をともに実行する場合には、偽レスポンスDB133に、不正なレスポンスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンス（例えば、偽のディレクトリ情報など）を格納することとなる。

#### 【0208】

ただし、上記実施の形態4で説明した統計に基づくフィルタリング処理をともに実施する場合には、かかるフィルタリング処理により破棄されたHTTPレスポンスについては、偽レスポンスを作成しないようにすることも有効である。このようなサーバダウンを狙ったHTTPレスポンスに対して偽レスポンスを作成したのでは、偽レスポンス作成処理の負担が却って増大してしまうからである。

#### 【0209】

(実施の形態9)

ところで、上記実施の形態8では、Webサーバ40に対する不正アクセスのパターンに対応する偽のレスポンスを格納した偽レスポンスDB133を参照して、偽レスポンスを作成する場合を説明したが、本発明はこれに限定されるものではなく、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストを受け入れて、Webサーバ40のおとりとして機能する偽Webサーバによって、偽のレスポンスを作成することもできる。

#### 【0210】

すなわち、Webサーバ40に対する不正アクセスには、パターンとして把握できないものもあり、このような不正アクセスについては、上記実施の形態8で説明した偽レスポンスDB133を参照して偽レスポンスを作成することできない。このため、不正アクセスが失敗したことを攻撃者に気づかせることなく時間を稼ぐこともできず、さらに、新たな別の不正アクセスを未然に防止したり、攻撃者の攻撃手口を解析することもできなくなってしまう。

#### 【0211】

そこで、本実施の形態9では、偽レスポンスDB133ではなく、不正なアクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストを受け入れて、Webサーバ40のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する偽Webサーバを導入することによって

、パターンとして把握できない不正アクセスに対しても、偽のレスポンスを送信することができるようしている。以下、本実施の形態9に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態9によるフィルタリングの処理手順とを説明する。

#### 【0212】

図16は、本実施の形態9に係るサーバクライアントシステムの構成を示すブロック図である。なお、図14に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態9の特徴部分である偽Webサーバ142について説明する。

#### 【0213】

サーバ装置140におけるリクエストフィルタ141の偽Webサーバ142は、不正なアクセスとしてWebサーバ40に受け渡されなかつたHTTPリクエストを受け入れて、Webサーバ40のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する処理部である。具体的には、Webサーバ40と同様、HTTPリクエストに応じてHTML(HyperText Markup Language)などのマークアップ言語により記述された各種の情報を送信するなどのサービスをクライアント装置10に提供するものであるが、Webサーバ40のおとりとして、偽のサービスを提供(偽のレスポンスを作成)するように偽のデータを所有する。

#### 【0214】

例えば、Webサーバ40上のパスワードファイルをリクエストする不正なHTTPリクエストを受け入れて、偽のパスワードファイルを作成したり、コマンド文字列を含んだリクエストによりWebサーバ40上で任意のシステムコマンドを実行するなどの不正なHTTPリクエストを受け入れて、そのシステムコマンドを実行したり、Webサーバ40上に存在しないファイルをリクエストしてWebサーバ40の機能を停止させる不正なHTTPリクエストを受け入れて、その機能を停止させる処理などをおこなう。

#### 【0215】

すなわち、偽Webサーバ142は、不正なHTTPリクエストを受け入れて

、そのH T T Pリクエストに応じた処理を実行するものであるが、W e bサーバ4 0のおとりとして偽のデータを所有するものであるため、偽W e bサーバ1 4 2からのレスポンスは、不正なH T T Pリクエストを受け入れたW e bサーバ4 0からのレスポンスと同様のものであるが、偽のレスポンスとなる。

## 【0216】

次に、本実施の形態9によるフィルタリングの処理手順について説明する。図1 7は、本実施の形態9によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置1 4 0におけるリクエストフィルタ1 4 1は、クライアント装置1 0からのH T T PリクエストをW e bサーバ4 0が受信する前に受信して（ステップS 1 7 0 1）、上記実施の形態8によるフィルタリング処理と同様の処理（図1 5に示したステップS 1 5 0 1～S 1 5 0 8）を実行する（ステップS 1 7 0 1～ステップS 1 7 0 8）。

## 【0217】

このステップS 1 7 0 8に示すように、リクエストフィルタ1 4 1の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなうと（ステップS 1 7 0 8）、続いて、送信部3 5は、不正アクセスとしてW e bサーバ4 0に受け渡されなかったH T T Pリクエストを、偽W e bサーバ1 4 2に送信する（ステップS 1 7 0 9）。

## 【0218】

そして、偽W e bサーバ1 4 2は、W e bサーバ4 0のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する（ステップS 1 7 1 0）。具体的には、W e bサーバ4 0上のパスワードファイルをリクエストする不正なH T T Pリクエストを受け入れて、偽のパスワードファイルを作成したり、コマンド文字列を含んだリクエストによりW e bサーバ4 0上で任意のシステムコマンドを実行するなどの不正なH T T Pリクエストを受け入れて、そのシステムコマンドを実行したりなどする。その後、レスポンス送信部1 3 4は、偽W e bサーバ1 4 2により作成された偽のレスポンスをクライアント装置1 0に送信する（ステップS 1 7 1 1）。

## 【0219】

上記した一連の処理によって、不正アクセスのパターンとして把握できないHTTPリクエストをWebサーバ40に送信してきたクライアント装置10に対しても、不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを送信されることとなる。

#### 【0220】

上述してきたように、本実施の形態9によれば、不正なアクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストを受け入れて、Webサーバ40のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する偽Webサーバ142を導入することとしたので、パターンとして把握できない不正アクセスに対しても、偽のレスポンスを送信することができる。特に、上記実施の形態8で説明したおとりシステムと異なり、偽Webサーバ142は、不正アクセスから保護したいWebサーバ40のミラーサーバ若しくはテストサーバを装って運用される必要がないので、実質的にWebサーバ40のおとりになれる点でも有効であると考えられる。

#### 【0221】

なお、本実施の形態9においても、クライアント装置10から送信されたHTTPリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態8と同様、上記実施の形態3で説明した事前判定処理や、上記実施の形態4で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態6で説明したレスポンスのフィルタリング処理とともに実行する場合にも同様に適用することができる。

#### 【0222】

##### (実施の形態10)

ところで、上記実施の形態8および9では、Webサーバ40に受け渡されなかった不正なHTTPリクエストのパターンに対応した偽のレスポンスを作成する場合と、不正なHTTPリクエストを受け入れて、Webサーバ40のおとりとして偽のレスポンスを作成する場合とを説明したが、本発明はこれに限定されるものではなく、これらの両者をともに実行する場合にも同様に適用することが

できる。

#### 【0223】

すなわち、上記実施の形態9では、Webサーバ40に受け渡されなかった不正なHTTPリクエストの全てを偽Webサーバ142に受け渡すことによって、偽のレスポンスを作成することとしたが、不正アクセスのパターンとして把握できる不正なHTTPリクエストについても偽Webサーバ142に受け渡したのでは、偽Webサーバ142に過度な負担が強いられることとなる。

#### 【0224】

そこで、本実施の形態10では、不正アクセスのパターンとして把握できる不正なHTTPリクエストについては、不正レスポンスDB133を参照して偽レスポンスを作成する一方、不正アクセスのパターンとして把握できない不正なHTTPリクエストについては、偽Webサーバ142により偽レスポンスを作成することとし、偽レスポンスを効率的かつ迅速に作成することができるようしている。以下、本実施の形態10に係るサーバクライアントシステムにおけるサーバ装置の構成と、本実施の形態10によるフィルタリングの処理手順とを説明する。

#### 【0225】

図18は、本実施の形態10に係るサーバクライアントシステムの構成を示すブロック図である。なお、図14または16に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態10の特徴部分である偽レスポンス作成部152について説明する。

#### 【0226】

サーバ装置150におけるリクエストフィルタ151の偽レスポンス作成部152は、偽レスポンスDB133および所定の作成ルール152aに基づいて、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストのパターンに対応した偽のレスポンスを作成するとともに、偽のレスポンスが作成できなかったHTTPリクエストを偽Webサーバ142に受け渡す処理部である。

#### 【0227】

具体的には、偽レスポンス作成部152は、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストを送信部35から受け付け、このHTTPリクエストのパターンが偽レスポンスDB133に格納されている不正リクエストのパターンに該当するか否かを判定する。そして、このパターンに該当する場合には、上記実施の形態8と同様、偽レスポンスDB133に基づいて偽レスポンスを作成する。一方、このパターンに該当しない場合には、HTTPリクエストを偽Webサーバ142に受け渡し、偽Webサーバ142に、上記実施の形態9の同様、Webサーバ40のおとりとして偽レスポンスを作成させる。

#### 【0228】

次に、本実施の形態10によるフィルタリングの処理手順について説明する。図19は、本実施の形態10によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置150におけるリクエストフィルタ151は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信して（ステップS1901）、上記実施の形態8によるフィルタリング処理と同様の処理（図15に示したステップS1501～S1508）を実行する（ステップS1901～ステップS1908）。

#### 【0229】

このステップS1908に示すように、リクエストフィルタ151の各部は、不正リクエストの破棄、格納媒体への格納、外部装置への通報などの不正判定時の処理をおこなうと（ステップS1908）、続いて、偽レスポンス作成部152は、破棄されたHTTPリクエストのパターンが偽レスポンスDB133に格納されている不正リクエストのパターンに該当するか否かを判定する（ステップS1909）。

#### 【0230】

この判定により、不正リクエストのパターンに該当する場合には（ステップS1909肯定）、偽レスポンス作成部152は、偽レスポンスDB133および所定の作成ルール152aに基づいて、不正アクセスとしてWebサーバ40に受け渡されなかったHTTPリクエストのパターンに対応した偽のレスポンスを

作成する（ステップS1910）。そして、レスポンス送信部134は、偽レスポンス作成部152により作成された偽のレスポンスをクライアント装置10に送信する（ステップS1911）。

#### 【0231】

これとは反対に、不正リクエストのパターンに該当しない場合には（ステップS1909否定）偽レスポンス作成部152は、パターンに該当しなかったHTTPリクエストを偽Webサーバ142に送信する（ステップS1912）。そして、偽Webサーバ142は、Webサーバ40のおとりとして該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを作成する（ステップS1913）。その後、レスポンス送信部134は、偽Webサーバ142により作成された偽のレスポンスをクライアント装置10に送信する（ステップS1911）。

#### 【0232】

上記した一連の処理によって、不正アクセスのパターンとして把握できる不正なHTTPリクエストについては、不正レスポンスDB133を参照して偽レスポンスが作成される一方、不正アクセスのパターンとして把握できない不正なHTTPリクエストについては、偽Webサーバ142により偽レスポンスが作成されることとなる。

#### 【0233】

上述してきたように、本実施の形態10によれば、不正アクセスのパターンとして把握できる不正なHTTPリクエストについては、不正レスポンスDB133を参照して偽レスポンスを作成する一方、不正アクセスのパターンとして把握できない不正なHTTPリクエストについては、偽Webサーバ142により偽レスポンスを作成することとしたので、偽Webサーバ142に過度な負担を強いることなく、偽レスポンスを効率的かつ迅速に作成することができる。

#### 【0234】

なお、本実施の形態10においても、クライアント装置10から送信されたHTTPリクエストに対しては、パターンに基づくフィルタリング処理を実行する場合を説明したが、本発明はこれに限定されるものではなく、上記実施の形態8

および9と同様、上記実施の形態3で説明した事前判定処理や、上記実施の形態4で説明した統計に基づくフィルタリング処理、さらには、上記実施の形態6で説明したレスポンスのフィルタリング処理とともに実行する場合にも同様に適用することができる。

#### 【0235】

##### (他の実施の形態)

さて、これまで本発明の実施の形態について説明したが、本発明は上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてもよいものである。

#### 【0236】

例えば、本実施の形態4～10では、クライアント装置10からのHTTPリクエストをフィルタリングする場合について説明したが、本発明はこれに限定されるものではなく、FTP(File Transfer Protocol)、telnet、コンソールなど、クライアント装置10からWebサーバ40に入力されるあらゆる情報をフィルタリングする場合に同様に適用することができる。

#### 【0237】

また、本実施の形態4～10では、フィルタリング装置としてのリクエストフィルタをサーバ装置に設けた場合について説明したが、本発明はこれに限定されるものではなく、例えば、それぞれのクライアント装置側にリクエストフィルタを設けたり、一つのリクエストフィルタにより複数のWebサーバを防御するなど、クライアント装置とWebサーバとの間にリクエストフィルタが介在するあらゆるシステム構成において同様に適用することができる。

#### 【0238】

なお、本実施の形態4～10で説明したフィルタリング方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク(FD)、CD-ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コン

ピュータによって記録媒体から読み出されることによって実行することもできる。

#### 【0239】

(付記1) クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の第1の見積ルールに基づいて前記アクセス要求の正当性を見積もる第1の見積手段と、

前記第1の見積手段による見積結果および所定の第1の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第1の判定手段と、

を備えたことを特徴とするフィルタリング装置。

#### 【0240】

(付記2) 前記第1の見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第1の判定手段は、前記第1の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第1の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記1に記載のフィルタリング装置。

#### 【0241】

(付記3) 前記第1の見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記第1の判定手段は、前記第1の見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを

判定することを特徴とする付記1に記載のフィルタリング装置。

【0242】

(付記4) 前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースと、前記第1の見積手段による正当性の見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記第1の見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記1、2または3に記載のフィルタリング装置。

【0243】

(付記5) 所定の第1の外部送信ルールに基づいて、前記第1の判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する第1の外部送信手段をさらに備えたことを特徴とする付記1～4のいずれか一つに記載のフィルタリング装置。

【0244】

(付記6) 所定の第1の格納ルールに基づいて、前記第1の判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する第1の格納手段をさらに備えたことを特徴とする付記1～5のいずれか一つに記載のフィルタリング装置。

【0245】

(付記7) 所定の第1の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、第1の見積ルール、第1の判定ルール、第1の外部送信ルール、第1の格納ルールまたは第1の更新ルールを更新する第1の更新手段をさらに備えたことを特徴とする付記1～6のいずれか一つに記載のフィルタリング装置。

【0246】

(付記8) 前記サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正データベースと、前記統計的不正データベースに格納された情報および所定の第2の見積ルールに基づい

て前記アクセス要求の正当性を見積もる第2の見積手段と、前記見積手段による見積結果および所定の第2の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第2の判定手段と、前記第1および第2の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみを正当なアクセス要求として前記サーバに受け渡すアクセス要求受渡手段と、をさらに備えたことを特徴とする付記1～7のいずれか一つに記載のフィルタリング装置。

## 【0247】

(付記9) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するものであって、

前記第2の見積手段は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第2の判定手段は、前記第2の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第2の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記8に記載のフィルタリング装置。

## 【0248】

(付記10) 前記統計的不正データベースは、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第2の見積手段は、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第2の判定手段は、前記第2の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サー

バに受け渡さないものと判定するとともに、前記第2の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記8に記載のフィルタリング装置。

#### 【0249】

(付記11) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第2の見積手段は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合または前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合および前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第2の判定手段は、前記第2の見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第2の見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記8に記載のフィルタリング装置。

#### 【0250】

(付記12) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第2の見積手段は、前記アクセス要求の送信元情報および要求内容が前記統計的不正データベースに格納された送信元情報および要求内容に該当する度合

に応じて所定の見積値を算出し、前記第2の判定手段は、前記第2の見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記8に記載のフィルタリング装置。

【0251】

(付記13) 前記第2の見積手段は、前記第1の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記8～12のいずれか一つに記載のフィルタリング装置。

【0252】

(付記14) 前記第1の見積手段は、前記第2の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記8～12のいずれか一つに記載のフィルタリング装置。

【0253】

(付記15) 前記事前判定手段は、前記第2の判定手段により前記サーバに受け渡すものと判定されたアクセス要求のみについて前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定することを特徴とする付記8～12のいずれか一つに記載のフィルタリング装置。

【0254】

(付記16) 所定の第2の外部送信ルールに基づいて、前記アクセス要求受渡手段により前記サーバに受け渡されなかったアクセス要求を所定の外部装置に送信する第2の外部送信手段をさらに備えたことを特徴とする付記8～15のいずれか一つに記載のフィルタリング装置。

【0255】

(付記17) 所定の第2の格納ルールに基づいて、前記アクセス要求受渡手段により前記サーバに受け渡されなかったアクセス要求を所定の格納媒体に格納する第2の格納手段をさらに備えたことを特徴とする付記8～16のいずれか一つに記載のフィルタリング装置。

【0256】

(付記18) 所定の第2の更新ルールおよび／または前記サーバに対するアクセ

ス要求の統計に基づいて、前記統計的不正データベース、第2の見積ルール、第2の判定ルール、第2の外部送信ルール、第2の格納ルールおよび／または第2の更新ルールを更新する第2の更新手段をさらに備えたことを特徴とする付記8～17のいずれか一つに記載のフィルタリング装置。

【0257】

(付記19) 前記第2の更新手段は、所定時間内に前記サーバに対してアクセス要求を送信した各クライアントごとのアクセス要求数および／または所定時間内に前記サーバに対して送信されたアクセス要求の各要求内容ごとのアクセス要求数に応じて、前記統計的不正データベースに格納される送信元情報および／または要求内容を追加および／または削除することを特徴とする付記18に記載のフィルタリング装置。

【0258】

(付記20) 前記アクセス要求に応じて前記サーバから前記クライアントに対して前記サービスとして送信されるレスポンスのうち、前記クライアントに対して送信されるべきでない不正レスポンスのパターンを格納した不正レスポンスデータベースと、前記不正レスポンスデータベースに格納された不正レスポンスのパターンおよび所定のレスポンス見積ルールに基づいて前記レスポンスの正当性を見積もるレスポンス見積手段と、前記レスポンス見積手段による見積結果および所定のレスponsス判定ルールに基づいて前記レスポンスを前記クライアントに送信するか否かを判定するレスポンス判定手段と、前記レスポンス判定手段により前記クライアントに送信するものと判定されたレスポンスのみを正当なレスポンスとして前記クライアントに送信するレスポンス送信手段と、をさらに備えたことを特徴とする付記1～19のいずれか一つに記載のフィルタリング装置。

【0259】

(付記21) 前記レスポンス見積手段は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれかに該当する場合に該レスポンスは不正レスポンスである旨を見積もるとともに、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれにも該当しない場合に該レスポンスは正当レスポンスである旨を見積もり、

前記レスポンス判定手段は、前記レスポンス見積手段により不正レスポンスである旨が見積もられたレスポンスを前記クライアントに送信しないものと判定するとともに、前記レスポンス見積手段により正当レスポンスである旨が見積もられたレスポンスを前記クライアントに送信するものと判定することを特徴とする付記20に記載のフィルタリング装置。

【0260】

(付記22) 前記レスポンス見積手段は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンに該当する度合に応じて所定の見積値を算出し、前記レスポンス判定手段は、前記レスポンス見積手段により算出された見積値と所定の閾値とを比較して前記レスポンスを前記クライアントに送信するか否かを判定することを特徴とする付記20に記載のフィルタリング装置。

【0261】

(付記23) 所定の第3の外部送信ルールに基づいて、前記レスポンス送信手段により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の外部装置に送信する第3の外部送信手段をさらに備えたことを特徴とする付記20、21または22に記載のフィルタリング装置。

【0262】

(付記24) 所定の第3の格納ルールに基づいて、前記レスポンス送信手段により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の格納媒体に格納する第3の格納手段をさらに備えたことを特徴とする付記20～23のいずれか一つに記載のフィルタリング装置。

【0263】

(付記25) 所定の第3の更新ルールに基づいて、前記不正レスポンスデータベース、レスポンス見積ルール、レスポンス判定ルール、第3の外部送信ルール、第3の格納ルールおよび／または第3の更新ルールを更新する第3の更新手段をさらに備えたことを特徴とする付記20～24のいずれか一つに記載のフィルタ

リング装置。

【0264】

(付記26) 所定の暗号処理がなされたアクセス要求を復号する第1の復号手段をさらに備え、前記第1の見積手段、事前判定手段または第2の見積手段は、前記第1の復号手段により復号されたアクセス要求について見積または判定をおこなうことを特徴とする付記1～25のいずれか一つに記載のフィルタリング装置。

【0265】

(付記27) 前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡す場合に、前記第1の復号手段により復号されたアクセス要求ではなく、所定の暗号処理がなされたアクセス要求を前記サーバに受け渡すことを特徴とする付記26に記載のフィルタリング装置。

【0266】

(付記28) 所定の暗号処理がなされたレスポンスを復号する第2の復号手段をさらに備え、前記レスポンス見積手段は、前記第2の復号手段により復号されたレスポンスについて見積をおこなうことを特徴とする付記26または27に記載のフィルタリング装置。

【0267】

(付記29) 前記レスポンスのうちの正当なレスポンスのみを前記クライアントに送信する場合に、前記第2の復号手段により復号されたレスポンスではなく、所定の暗号処理がなされたレスポンスを前記クライアントに送信することを特徴とする付記28に記載のフィルタリング装置。

【0268】

(付記30) 前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースと、前記偽レスポンスデータベースを参照して、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のパターンに対応した偽のレスポンスを作成する偽レスポンス作成手段と、前記偽レスポンス作成手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信

手段と、をさらに備えたことを特徴とする付記1～29のいずれか一つに記載のフィルタリング装置。

【0269】

(付記31) 不正なアクセスとして前記サーバに受け渡されなかったアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり手段と、前記おとり手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信手段と、をさらに備えたことを特徴とする付記1～29のいずれか一つに記載のフィルタリング装置。

【0270】

(付記32) 前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースと、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応するアクセス要求について該パターンに対応した偽のレスポンスを作成する偽レスポンス作成手段と、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応しないアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり手段と、前記偽レスポンス作成手段または前記おとり手段により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信手段と、をさらに備えたことを特徴とする付記1～29のいずれか一つに記載のフィルタリング装置。

【0271】

(付記33) クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の第1の見積ルー

ルに基づいて前記アクセス要求の正当性を見積もる第1の見積工程と、

前記第1の見積工程による見積結果および所定の第1の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第1の判定工程と、を含んだことを特徴とするフィルタリング方法。

#### 【0272】

(付記34) 前記第1の見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第1の判定工程は、前記第1の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第1の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記33に記載のフィルタリング方法。

#### 【0273】

(付記35) 前記第1の見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記第1の判定工程は、前記第1の見積工程により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記33に記載のフィルタリング方法。

#### 【0274】

(付記36) 前記第1の見積工程による正当性の見積もりの前に、前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定工程をさらに含み、前記第1の見積工程は、前記事前判定工程により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記33、34または35に記載のフィルタリング方法。

【0275】

(付記37) 所定の第1の外部送信ルールに基づいて、前記第1の判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する第1の外部送信工程をさらに含んだことを特徴とする付記33～36のいずれか一つに記載のフィルタリング方法。

【0276】

(付記38) 所定の第1の格納ルールに基づいて、前記第1の判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する第1の格納工程をさらに含んだことを特徴とする付記33～37のいずれか一つに記載のフィルタリング方法。

【0277】

(付記39) 所定の第1の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、第1の見積ルール、第1の判定ルール、第1の外部送信ルール、第1の格納ルールまたは第1の更新ルールを更新する第1の更新工程をさらに含んだことを特徴とする付記33～38のいずれか一つに記載のフィルタリング方法。

【0278】

(付記40) 前記サーバに対するアクセス要求の統計からみて不正アクセスとみなされるアクセス要求に関する情報を格納した統計的不正データベースを参照し、所定の第2の見積ルールに基づいて前記アクセス要求の正当性を見積もる第2の見積工程と、前記見積工程による見積結果および所定の第2の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する第2の判定工程と、前記第1および第2の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみを正当なアクセス要求として前記サーバに受け渡すアクセス要求受渡工程と、をさらに含んだことを特徴とする付記33～39のいずれか一つに記載のフィルタリング方法。

【0279】

(付記41) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えた

クライアントの送信元情報を格納するものであって、

前記第2の見積工程は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第2の判定工程は、前記第2の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第2の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記40に記載のフィルタリング方法。

#### 【0280】

(付記42) 前記統計的不正データベースは、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第2の見積工程は、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第2の判定工程は、前記第2の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第2の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記40に記載のフィルタリング方法。

#### 【0281】

(付記43) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第2の見積工程は、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれかに該当する場合または前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求の送信元情報が前記統計的不正データベースに格納された送信元情報のいずれにも該当しない場合および前記アクセス要求の要求内容が前記統計的不正データベースに格納された要求内容のいずれかにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記第2の判定工程は、前記第2の見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記第2の見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記40に記載のフィルタリング方法。

## 【0282】

(付記44) 前記統計的不正データベースは、前記サーバに対してアクセス要求を送信したクライアントのうち、所定時間内のアクセス要求数が所定数を超えたクライアントの送信元情報を格納するとともに、前記サーバに対して送信されたアクセス要求の要求内容のうち、所定時間内のアクセス要求数が所定数を超えた要求内容を格納するものであって、

前記第2の見積工程は、前記アクセス要求の送信元情報および要求内容が前記統計的不正データベースに格納された送信元情報および要求内容に該当する度合に応じて所定の見積値を算出し、前記第2の判定工程は、前記第2の見積工程により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記40に記載のフィルタリング方法。

## 【0283】

(付記45) 前記第2の見積工程は、前記第1の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記40～44のいずれか一つに記載のフィルタリング方法。

## 【0284】

(付記46) 前記第1の見積工程は、前記第2の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記40～44のいずれか一つに記載のフィルタリング方法。

【0285】

(付記47) 前記事前判定工程は、前記第2の判定工程により前記サーバに受け渡すものと判定されたアクセス要求のみについて前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定することを特徴とする付記40～44のいずれか一つに記載のフィルタリング方法。

【0286】

(付記48) 所定の第2の外部送信ルールに基づいて、前記アクセス要求受渡工程により前記サーバに受け渡されなかったアクセス要求を所定の外部装置に送信する第2の外部送信工程をさらに含んだことを特徴とする付記40～47のいずれか一つに記載のフィルタリング方法。

【0287】

(付記49) 所定の第2の格納ルールに基づいて、前記アクセス要求受渡工程により前記サーバに受け渡されなかったアクセス要求を所定の格納媒体に格納する第2の格納工程をさらに含んだことを特徴とする付記40～48のいずれか一つに記載のフィルタリング方法。

【0288】

(付記50) 所定の第2の更新ルールおよび／または前記サーバに対するアクセス要求の統計に基づいて、前記統計的不正データベース、第2の見積ルール、第2の判定ルール、第2の外部送信ルール、第2の格納ルールおよび／または第2の更新ルールを更新する第2の更新工程をさらに含んだことを特徴とする付記40～49のいずれか一つに記載のフィルタリング方法。

【0289】

(付記51) 前記第2の更新工程は、所定時間内に前記サーバに対してアクセス要求を送信した各クライアントごとのアクセス要求数および／または所定時間内に前記サーバに対して送信されたアクセス要求の各要求内容ごとのアクセス要求数に応じて、前記統計的不正データベースに格納される送信元情報および／また

は要求内容を追加および／または削除することを特徴とする付記50に記載のフィルタリング方法。

【0290】

(付記52) 前記アクセス要求に応じて前記サーバから前記クライアントに対して前記サービスとして送信されるレスポンスのうち、前記クライアントに対して送信されるべきでない不正レスポンスのパターンを格納した不正レスポンスデータベースを参照し、所定のレスポンス見積ルールに基づいて前記レスポンスの正当性を見積もるレスポンス見積工程と、前記レスポンス見積工程による見積結果および所定のレスポンス判定ルールに基づいて前記レスポンスを前記クライアントに送信するか否かを判定するレスポンス判定工程と、前記レスポンス判定工程により前記クライアントに送信するものと判定されたレスポンスのみを正当なレスポンスとして前記クライアントに送信するレスポンス送信工程と、をさらに含んだことを特徴とする付記33～51のいずれか一つに記載のフィルタリング方法。

【0291】

(付記53) 前記レスポンス見積工程は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれかに該当する場合に該レスポンスは不正レスポンスである旨を見積もるとともに、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンのいずれにも該当しない場合に該レスポンスは正当レスポンスである旨を見積もり、前記レスポンス判定工程は、前記レスポンス見積工程により不正レスポンスである旨が見積もられたレスポンスを前記クライアントに送信しないものと判定するとともに、前記レスポンス見積工程により正当レスポンスである旨が見積もられたレスポンスを前記クライアントに送信するものと判定することを特徴とする付記52に記載のフィルタリング方法。

【0292】

(付記54) 前記レスポンス見積工程は、前記レスポンスが前記不正レスポンスデータベースに格納された不正レスポンスのパターンに該当する度合に応じて所定の見積値を算出し、前記レスポンス判定工程は、前記レスポンス見積工程によ

り算出された見積値と所定の閾値とを比較して前記レスポンスを前記クライアントに送信するか否かを判定することを特徴とする付記52に記載のフィルタリング方法。

#### 【0293】

(付記55) 所定の第3の外部送信ルールに基づいて、前記レスポンス送信工程により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の外部装置に送信する第3の外部送信工程をさらに含んだことを特徴とする付記52、53または54に記載のフィルタリング方法。

#### 【0294】

(付記56) 所定の第3の格納ルールに基づいて、前記レスポンス送信工程により前記クライアントに送信されなかったレスポンスおよび／または該レスポンスの起因となったアクセス要求を所定の格納媒体に格納する第3の格納工程をさらに含んだことを特徴とする付記52～55のいずれか一つに記載のフィルタリング方法。

#### 【0295】

(付記57) 所定の第3の更新ルールに基づいて、前記不正レスポンスデータベース、レスポンス見積ルール、レスポンス判定ルール、第3の外部送信ルール、第3の格納ルールおよび／または第3の更新ルールを更新する第3の更新工程をさらに含んだことを特徴とする付記52～56のいずれか一つに記載のフィルタリング方法。

#### 【0296】

(付記58) 所定の暗号処理がなされたアクセス要求を復号する第1の復号工程をさらに含み、前記第1の見積工程、事前判定工程または第2の見積工程は、前記第1の復号工程により復号されたアクセス要求について見積または判定をおこなうことを特徴とする付記33～57のいずれか一つに記載のフィルタリング方法。

#### 【0297】

(付記59) 前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに

受け渡す場合に、前記第1の復号工程により復号されたアクセス要求ではなく、所定の暗号処理がなされたアクセス要求を前記サーバに受け渡すことを特徴とする付記58に記載のフィルタリング方法。

【0298】

(付記60) 所定の暗号処理がなされたレスポンスを復号する第2の復号工程をさらに含み、前記レスポンス見積工程は、前記第2の復号工程により復号されたレスポンスについて見積をおこなうことを特徴とする付記58または59に記載のフィルタリング方法。

【0299】

(付記61) 前記レスポンスのうちの正当なレスポンスのみを前記クライアントに送信する場合に、前記第2の復号工程により復号されたレスポンスではなく、所定の暗号処理がなされたレスポンスを前記クライアントに送信することを特徴とする付記60に記載のフィルタリング方法。

【0300】

(付記62) 前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを参照して、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のパターンに対応した偽のレスポンスを作成する偽レスポンス作成工程と、前記偽レスポンス作成工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記33～61のいずれか一つに記載のフィルタリング方法。

【0301】

(付記63) 不正なアクセスとして前記サーバに受け渡されなかったアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり工程と、前記おとり工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記33～61のいずれか一つに記載のフィルタリング方法。

【0302】

(付記64) 前記サーバに対する不正アクセスのパターンに対応付けて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを格納した偽レスポンスデータベースを参照し、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応するアクセス要求について該パターンに対応した偽のレスポンスを作成する偽レスポンス作成工程と、不正アクセスとして前記サーバに受け渡されなかったアクセス要求のうち、前記偽レスポンスデータベースに格納された不正アクセスのパターンに対応しないアクセス要求を受け入れて、該不正アクセスが成功若しくは進行している旨を示す偽のレスポンスを前記サーバのおとりとして作成するおとり工程と、前記偽レスポンス作成工程または前記おとり工程により作成された偽のレスポンスを前記クライアントに送信する偽レスポンス送信工程と、をさらに含んだことを特徴とする付記33～61のいずれか一つに記載のフィルタリング方法。

## 【0303】

(付記65) 前記付記33～64のいずれか一つに記載された方法をコンピュータに実行させるプログラム。

## 【0304】

## 【発明の効果】

以上説明したように、請求項1、8または9の発明によれば、サーバに対する不正アクセスのパターンを格納した不正パターンデータベースの不正アクセスのパターンおよび所定の見積ルールに基づいてアクセス要求の正当性を見積もり、この見積結果および所定の判定ルールに基づいてアクセス要求をサーバに受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみをサーバに受け渡すことができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができる。

## 【0305】

また、請求項2の発明によれば、アクセス要求が不正パターンデータベースに

格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、不正アクセスである旨が見積もられたアクセス要求をサーバに受け渡さないものと判定するとともに、正当アクセスである旨が見積もられたアクセス要求をサーバに受け渡すものと判定することとしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対しても迅速かつ確実にサーバを防御することができる。

#### 【0306】

また、請求項3の発明によれば、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、この算出された見積値と所定の閾値とを比較してアクセス要求をサーバに受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもある程度の幅を持ってサーバを防御することができる。

#### 【0307】

また、請求項4の発明によれば、正当性の見積もりの前に、サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、アクセス要求が正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定し、正当アクセスのパターンに該当しないものの判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくサーバに受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

#### 【0308】

また、請求項5の発明によれば、所定の外部送信ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信することとしたので、不正アクセスに関する情報をサーバの管理者、フィルタリング装置の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に送信することができ、もってかかる管理者に対しサーバの保全対策を迅速に促すことができる。

#### 【0309】

また、請求項6の発明によれば、所定の格納ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納することとしたので、格納媒体に格納された不正アクセスに関する情報を分析することなどができる、もってサーバの更なる保全対策を講じることができる。

#### 【0310】

また、請求項7の発明によれば、所定の更新ルールに基づいて、不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新することとしたので、新たに発見された不正アクセスのパターンを不正パターンデータベースに登録することなどができる、もって日々進化する不正アクセスに対して機動的に対応することができる

#### 【図面の簡単な説明】

##### 【図1】

本実施の形態1に係るサーバクライアントシステムの構成を示すブロック図である。

##### 【図2】

不正リクエストDBに格納される情報の構成例を示す図である。

##### 【図3】

本実施の形態1によるフィルタリングの処理手順を説明するフローチャートである。

##### 【図4】

本実施の形態2によるフィルタリングの処理手順を説明するフローチャートで

ある。

【図5】

本実施の形態3に係るサーバクライアントシステムの構成を示すブロック図である。

【図6】

本実施の形態3によるフィルタリングの処理手順を説明するフローチャートである。

【図7】

本実施の形態4に係るサーバクライアントシステムの構成を示すブロック図である。

【図8】

本実施の形態4によるフィルタリングの処理手順を説明するフローチャートである。

【図9】

本実施の形態4の変形例に係るサーバクライアントシステムの構成を示すブロック図である。

【図10】

本実施の形態5に係るサーバクライアントシステムの構成を示すブロック図である。

【図11】

本実施の形態6に係るサーバクライアントシステムの構成を示すブロック図である。

【図12】

本実施の形態6によるフィルタリングの処理手順を説明するフローチャートである。

【図13】

本実施の形態7に係るサーバクライアントシステムの構成を示すブロック図である。

【図14】

本実施の形態8に係るサーバクライアントシステムの構成を示すブロック図である。

【図15】

本実施の形態8によるフィルタリングの処理手順を説明するフローチャートである。

【図16】

本実施の形態9に係るサーバクライアントシステムの構成を示すブロック図である。

【図17】

本実施の形態9によるフィルタリングの処理手順を説明するフローチャートである。

【図18】

本実施の形態10に係るサーバクライアントシステムの構成を示すブロック図である。

【図19】

本実施の形態10に係るサーバクライアントシステムの構成を示すブロック図である。

【符号の説明】

- 1 ネットワーク
- 10 クライアント装置
- 11 Web ブラウザ
- 20、60 サーバ装置
- 30、70 リクエストフィルタ
- 31 受信部
- 32 見積部
- 32a 見積ルール
- 33 不正リクエストDB
- 34 判定部
- 34a 判定ルール

3 5 送信部  
3 6 ログ管理部  
3 6 a 管理ルール  
3 7 外部通報部  
3 7 a 通報ルール  
3 8 外部情報取得部  
3 8 a 取得ルール  
3 9 更新部  
3 9 a 更新ルール  
4 0 Webサーバ  
5 0 外部装置  
7 1 事前判定部  
7 1 a 事前判定ルール  
7 2 正当リクエストDB  
8 0、9 0 サーバ装置  
8 1、9 1 リクエストフィルタ  
8 2 第1見積部  
8 2 a 見積ルール  
8 3 不正リクエストDB  
8 4 第1判定部  
8 4 a 判定ルール  
8 5 第1見積部  
8 5 a 見積ルール  
8 6 統計的不正リクエストDB  
8 7 第2判定部  
8 7 a 判定ルール  
8 8 送信部  
1 0 0 サーバ装置  
1 0 1 リクエストフィルタ

102 アクセス管理部

103 動的更新部

103a 更新ルール

110、120 サーバ装置

111、121 リクエストフィルタ

112 レスポンス受信部

113 レスポンス見積部

113a 見積ルール

114 不正レスポンスDB

115 レスポンス判定部

115a 判定ルール

116 レスポンス送信部

122、123 復号部

130、140、150 サーバ装置

131、141、151 リクエストフィルタ

132、152 偽レスポンス作成部

132a、152a 作成ルール

133 偽レスポンスDB

134 レスポンス送信部

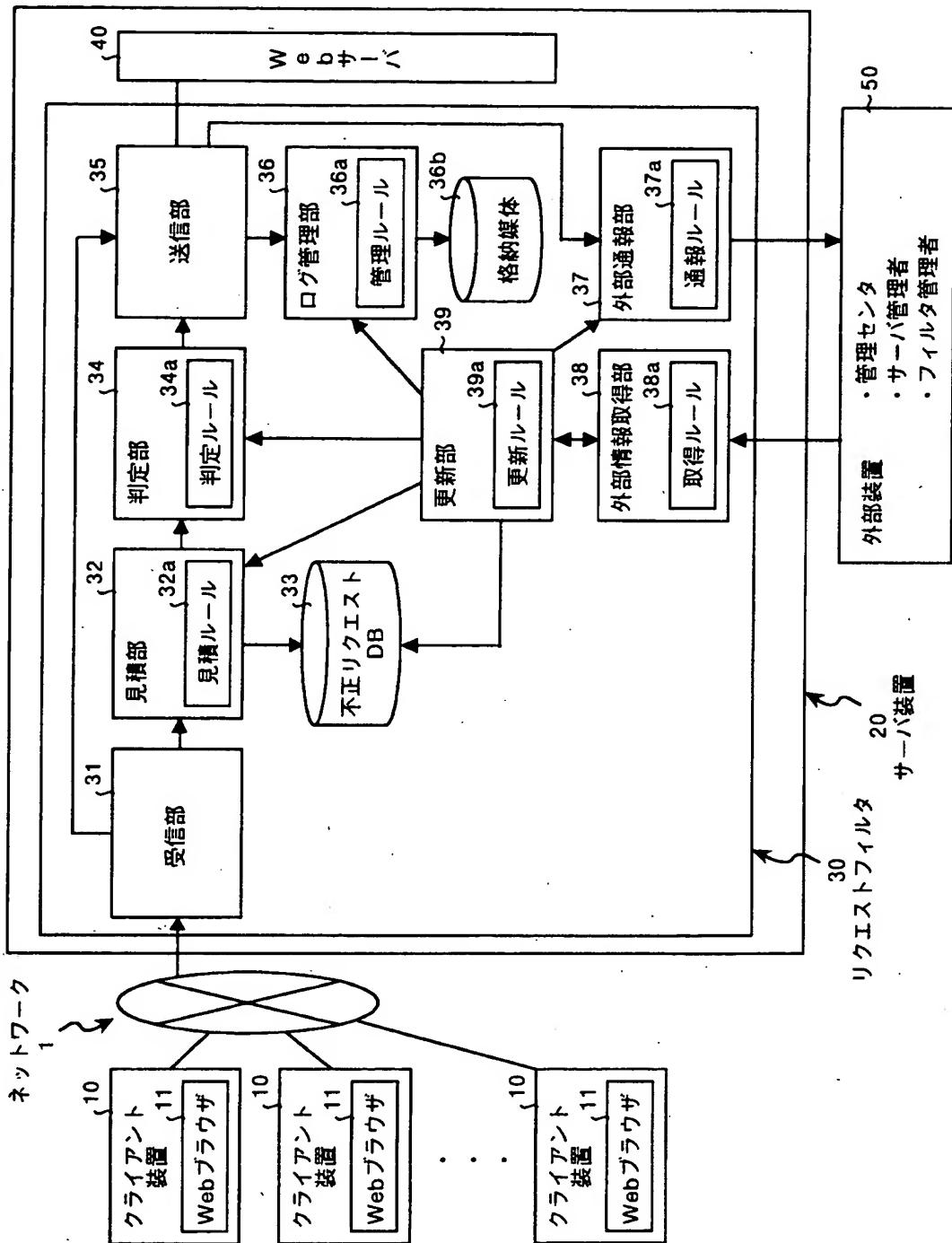
142 偽Webサーバ

【書類名】

図面

【図1】

本実施の形態1に係るサーバクライアントシステムの構成を示すブロック図



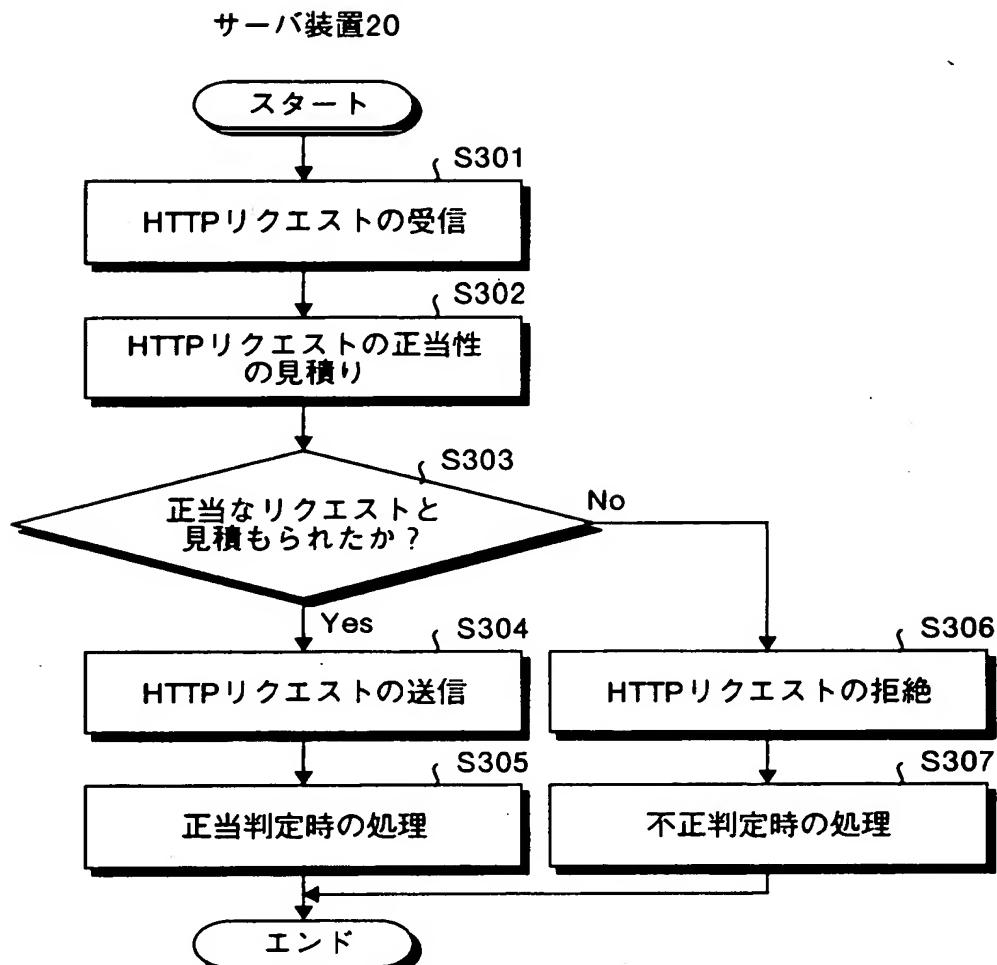
【図2】

## 不正リクエストDBに格納される情報の構成例を示す図

形式言語パターン	意味
URL=<//	URLの先頭が“//”と一致するリクエストを却下。
CGI==phf ARG=<Qname=root%OA	CGI名が“phf”であり、且つそのある引数の先頭が“Qname=root%OA”と一致するリクエストを却下。
URL<>...¥...¥...	URLに“¥¥¥...”が含まれるリクエストを却下。
CGI>=.htr	CGI名の末尾が“.htr”と一致するリクエストを却下。すなわち、CGIが拡張子“.htr”を有するリクエストを却下。

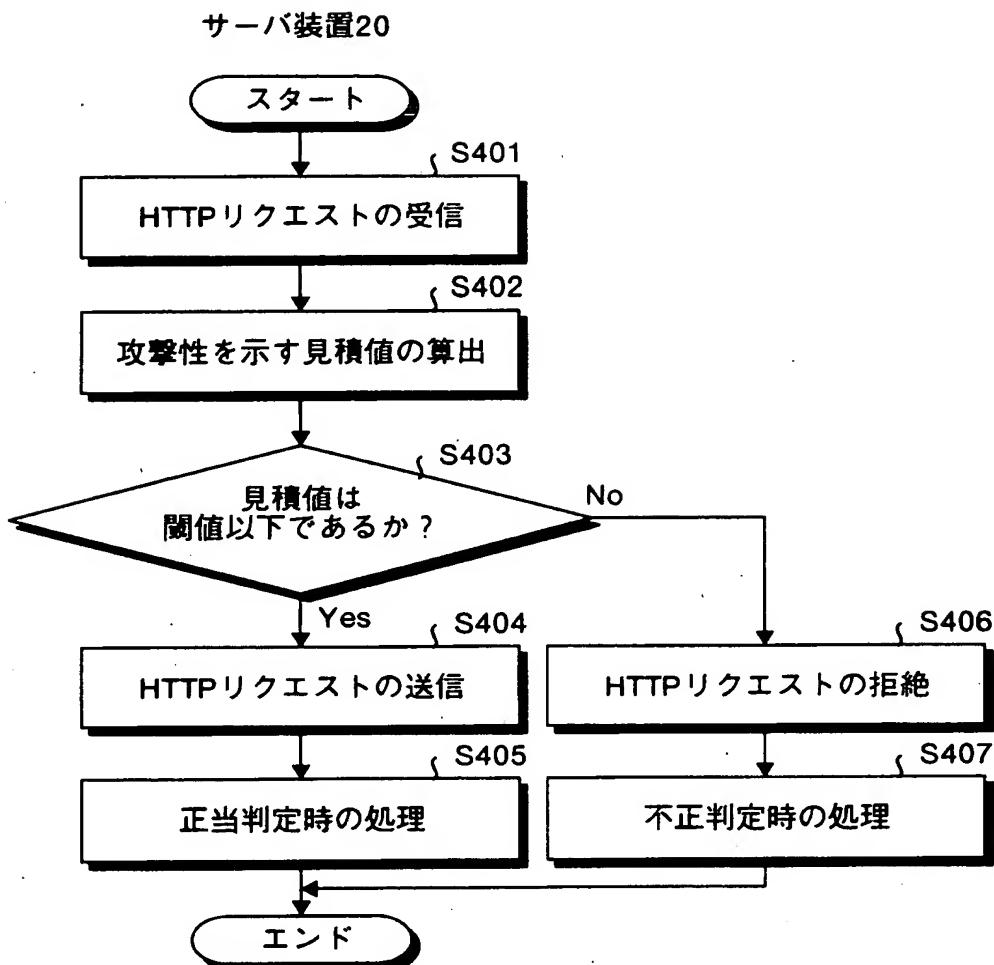
【図3】

本実施の形態1によるフィルタリングの処理手順を示すフローチャート



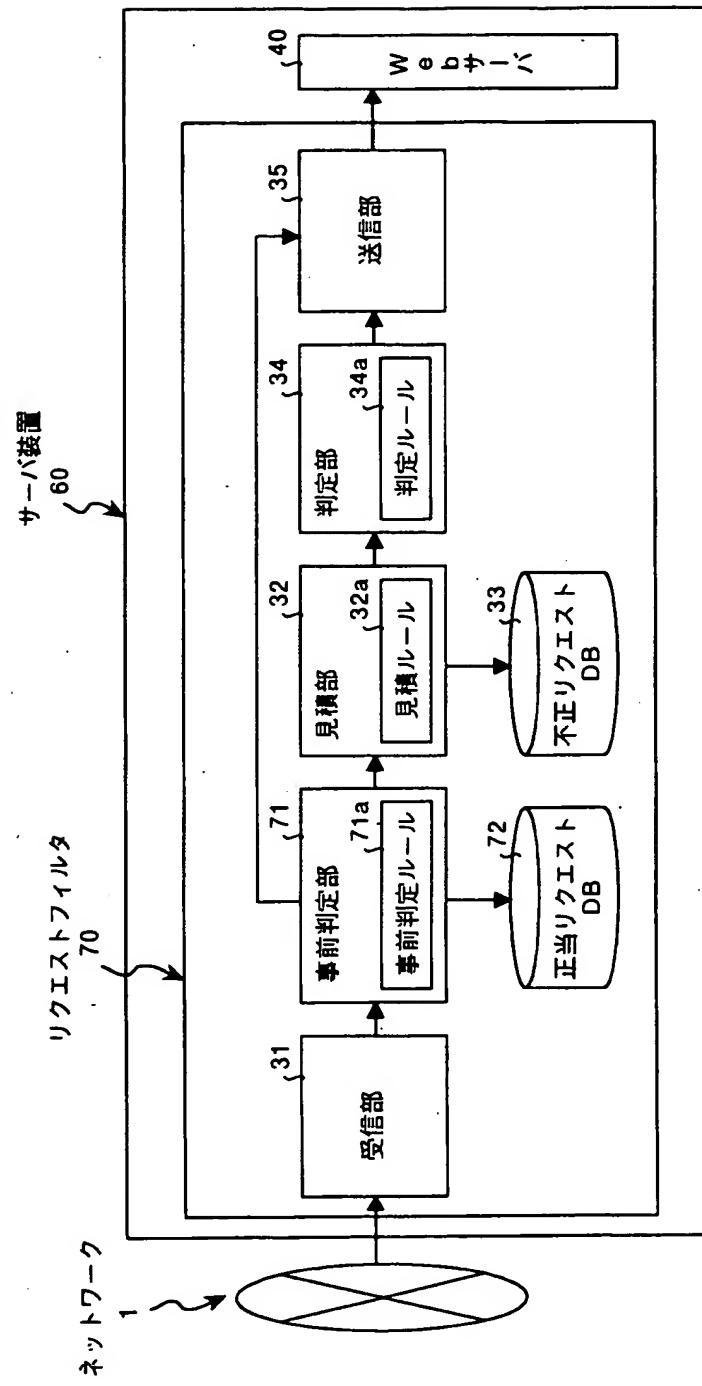
【図4】

本実施の形態2によるフィルタリングの処理手順を示すフローチャート



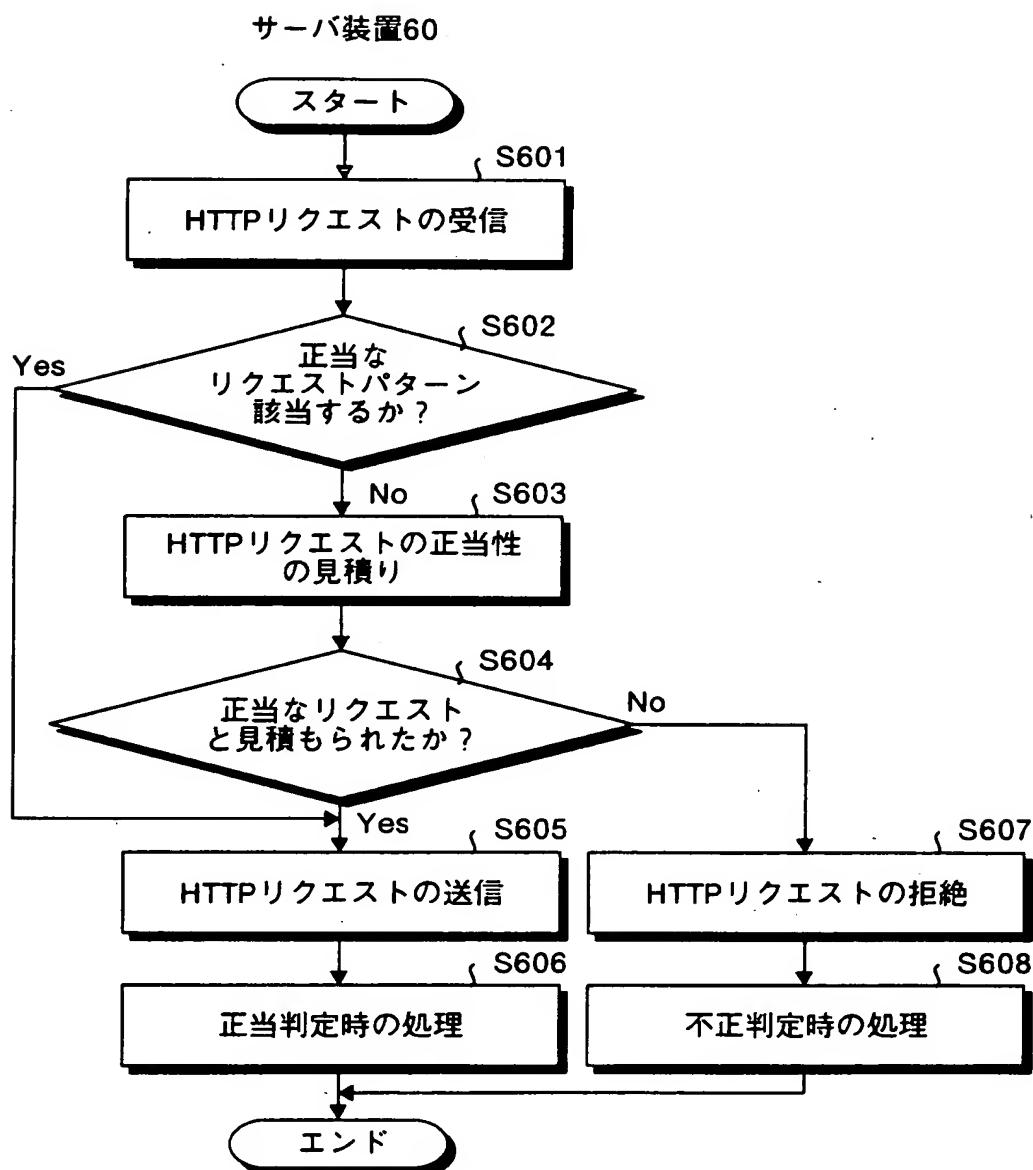
【図5】

本実施の形態3に係るサーバクライアントシステムの構成を示すブロック図



【図6】

本実施の形態3によるフィルタリングの処理手順を示すフローチャート

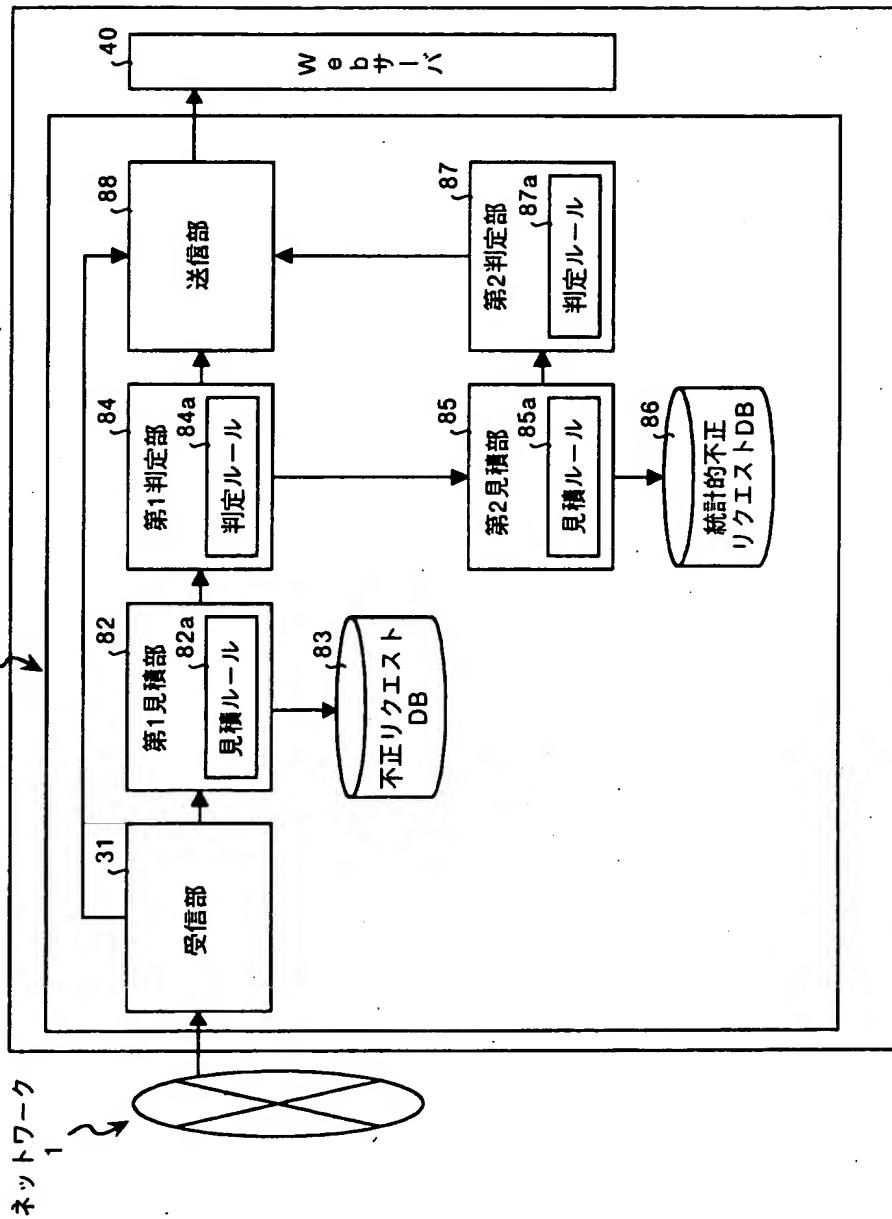


【図7】

本実施の形態4に係るサーバクライアントシステムの構成を示すブロック図

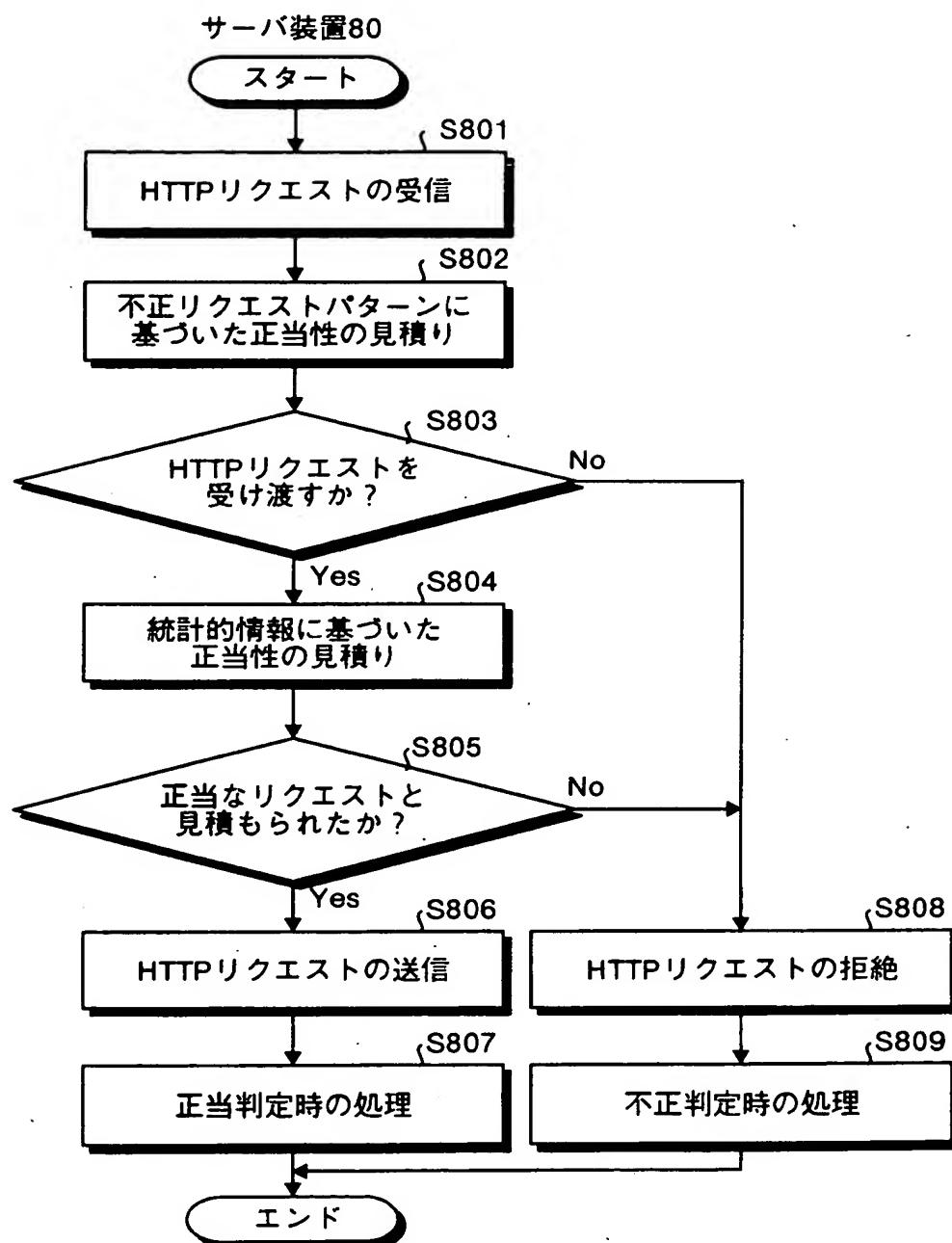
サーバ装置 80

リクエストフィルタ 81



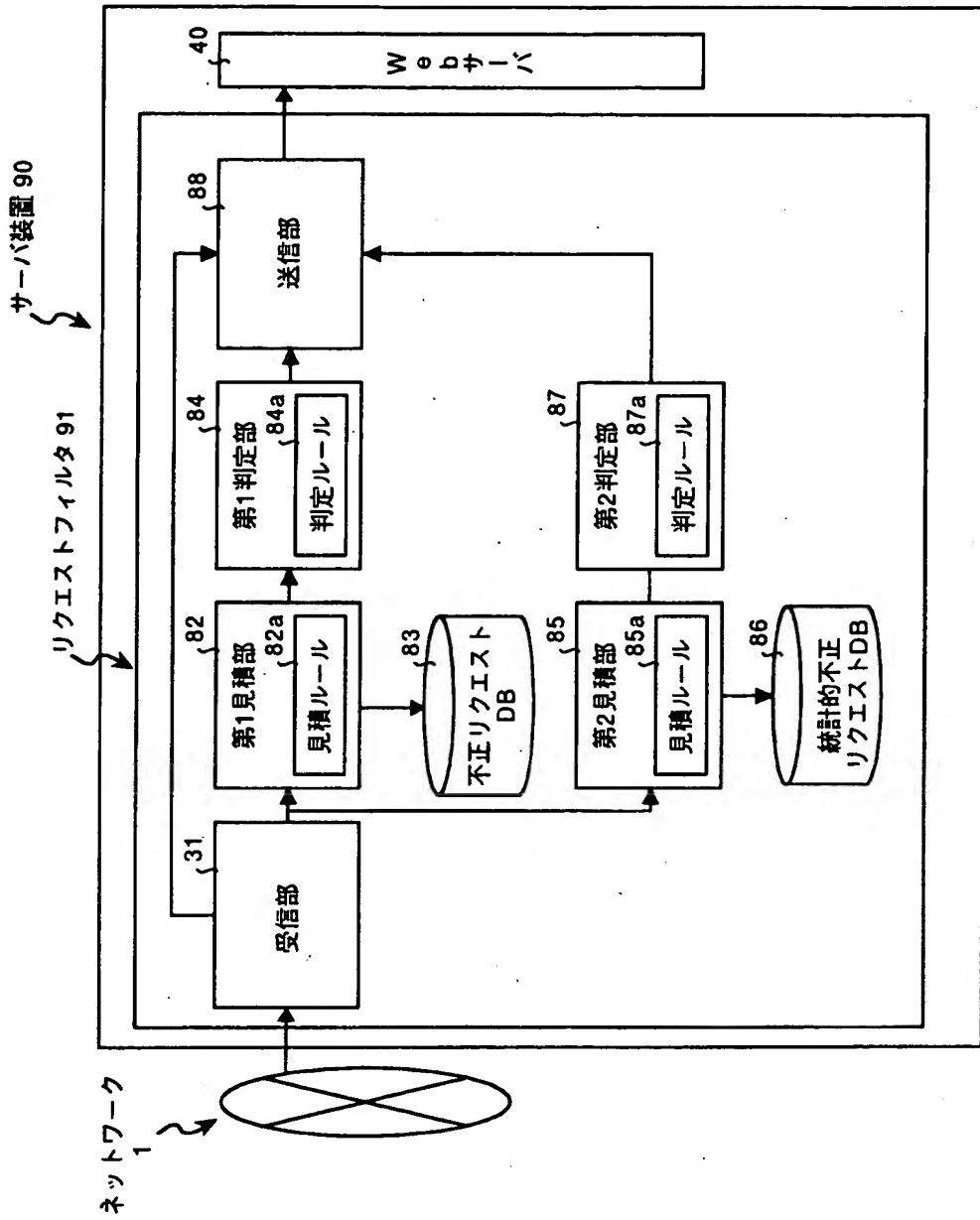
【図8】

本実施の形態4によるフィルタリングの処理手順を示すフローチャート



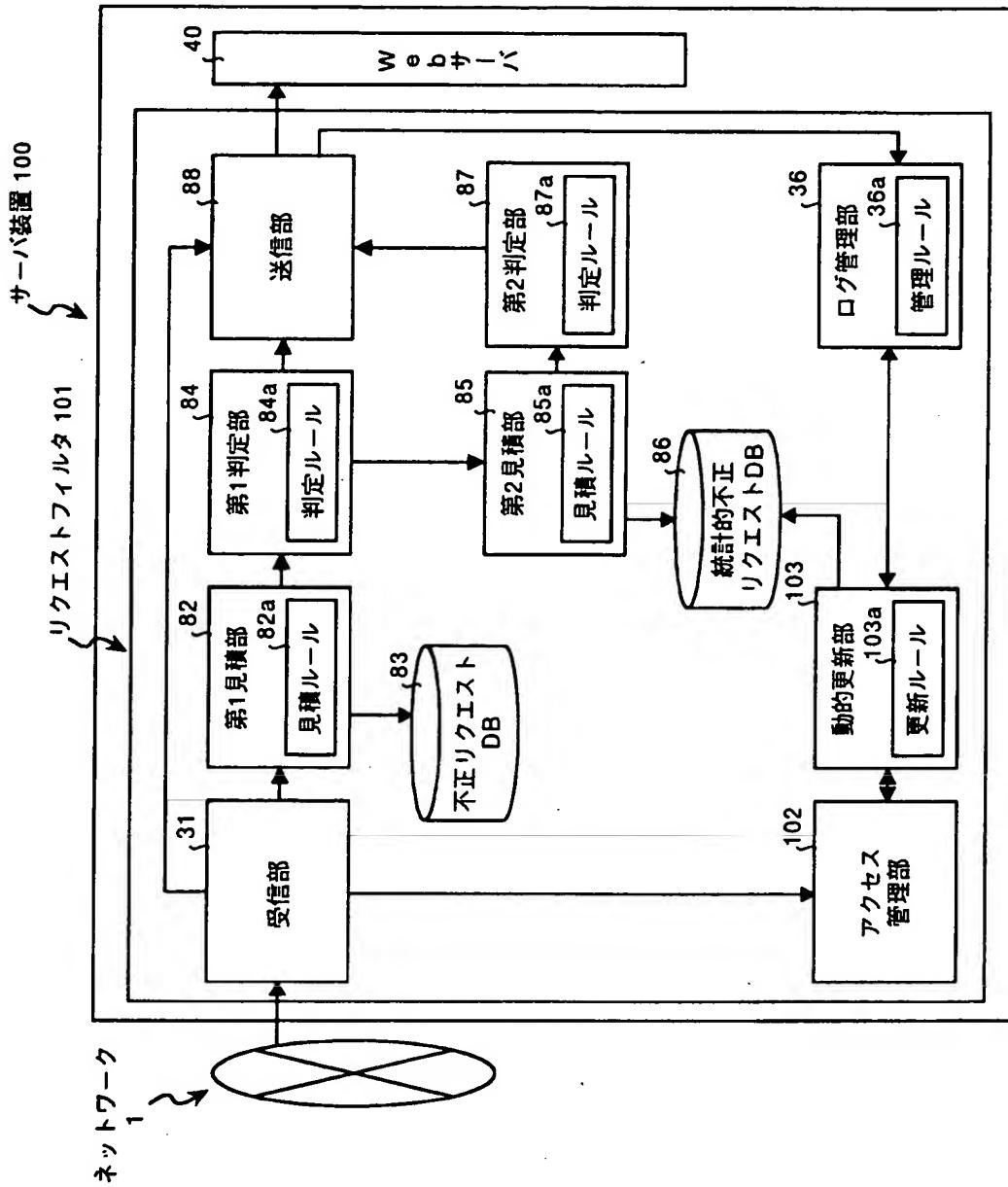
【図9】

本実施の形態4の変形例に係るサーバクライアントシステムの構成を示すブロック図



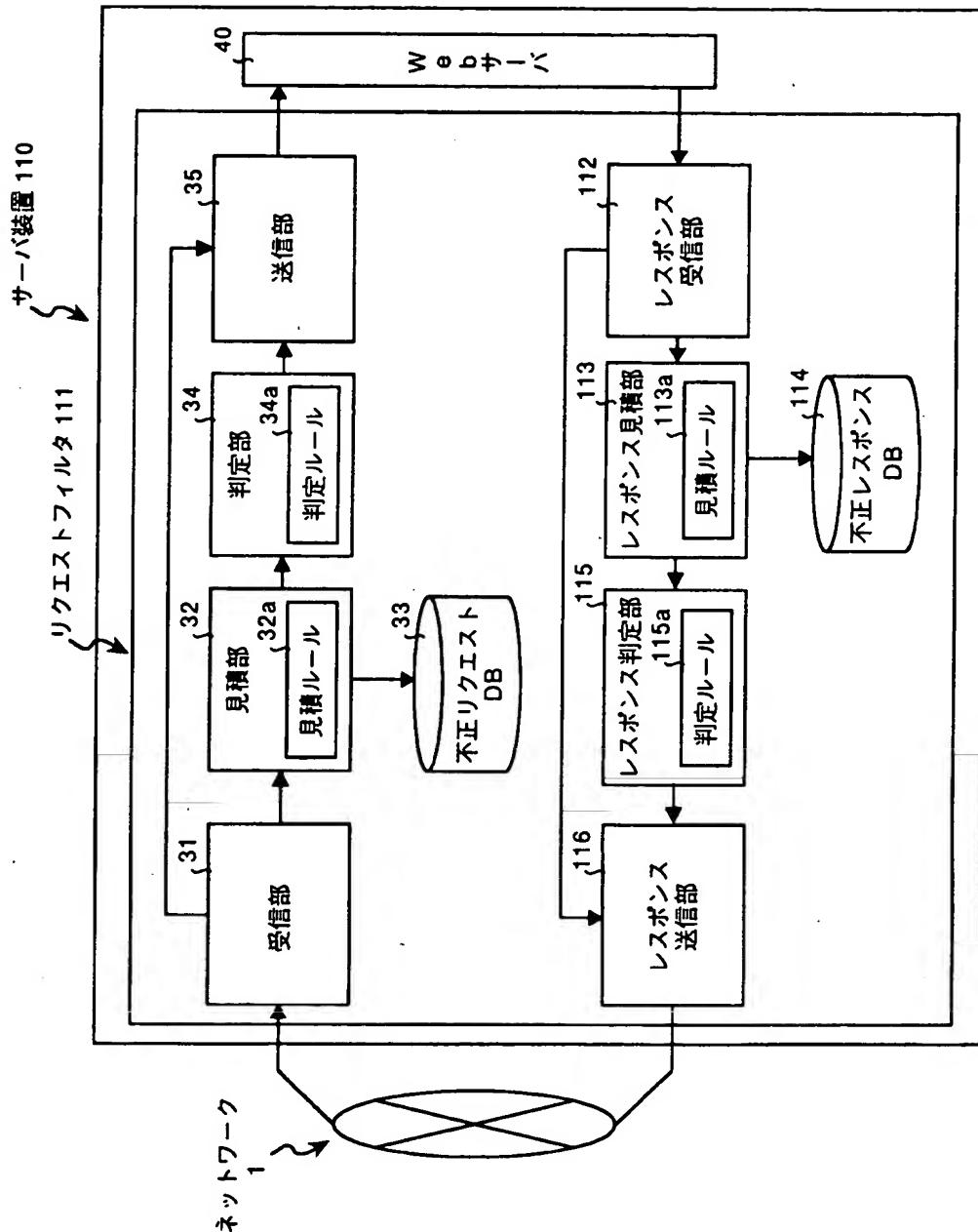
【図10】

本実施の形態5に係るサーバクライアントシステムの構成を示すプロック図



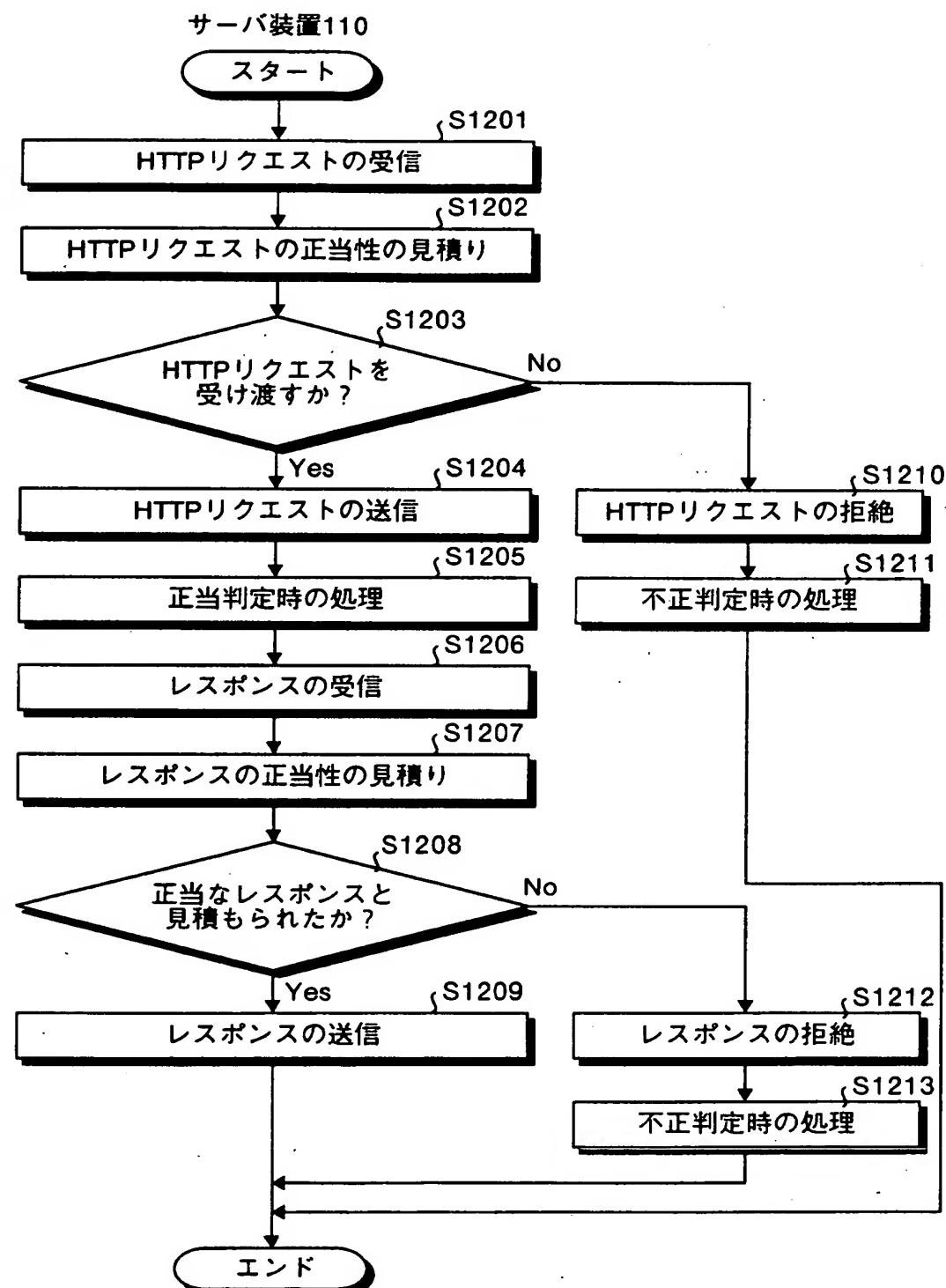
【図11】

本実施の形態6に係るサーバクライアントシステムの構成を示すブロック図



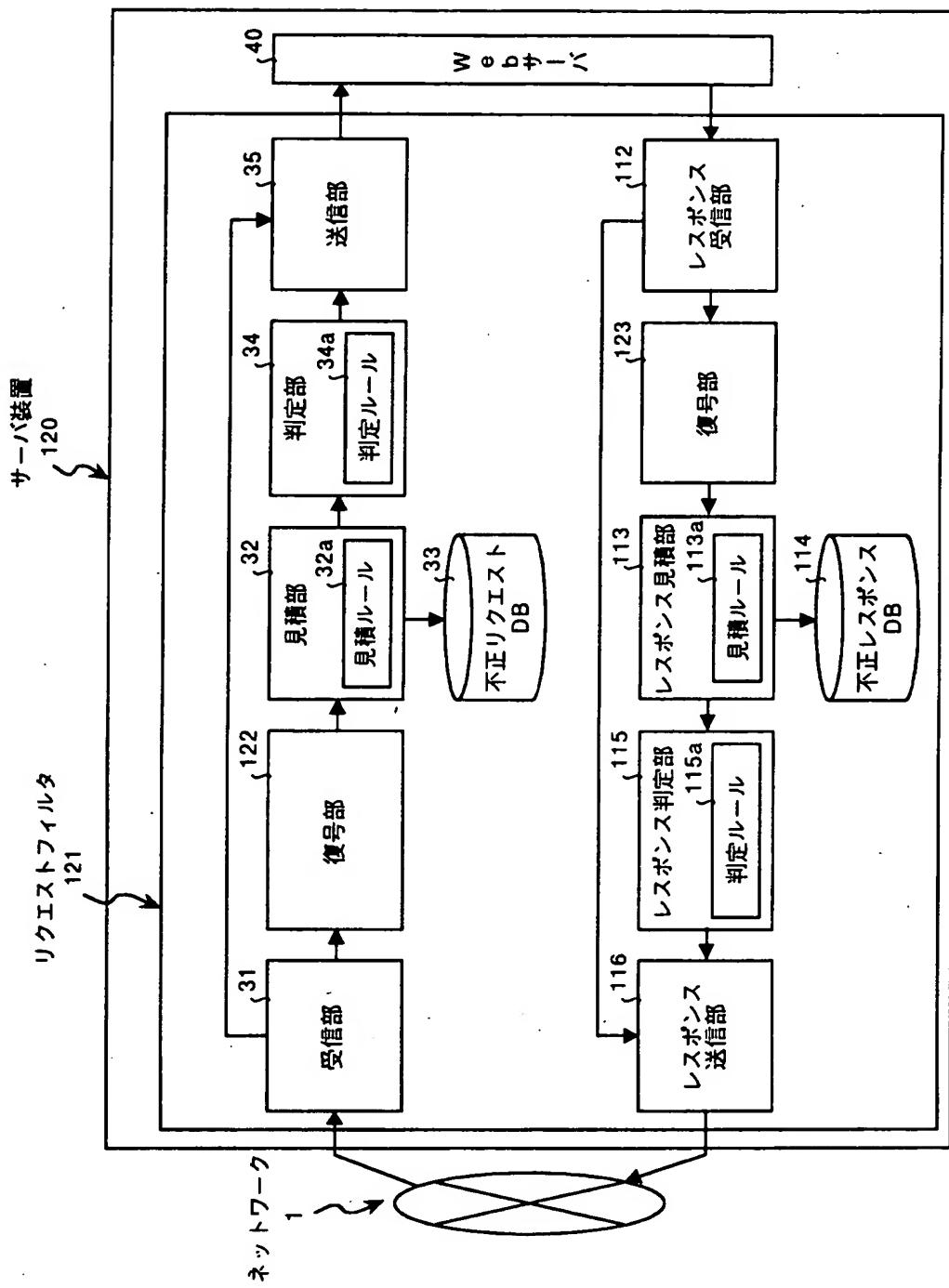
【図12】

本実施の形態6によるフィルタリングの処理手順を示すフローチャート



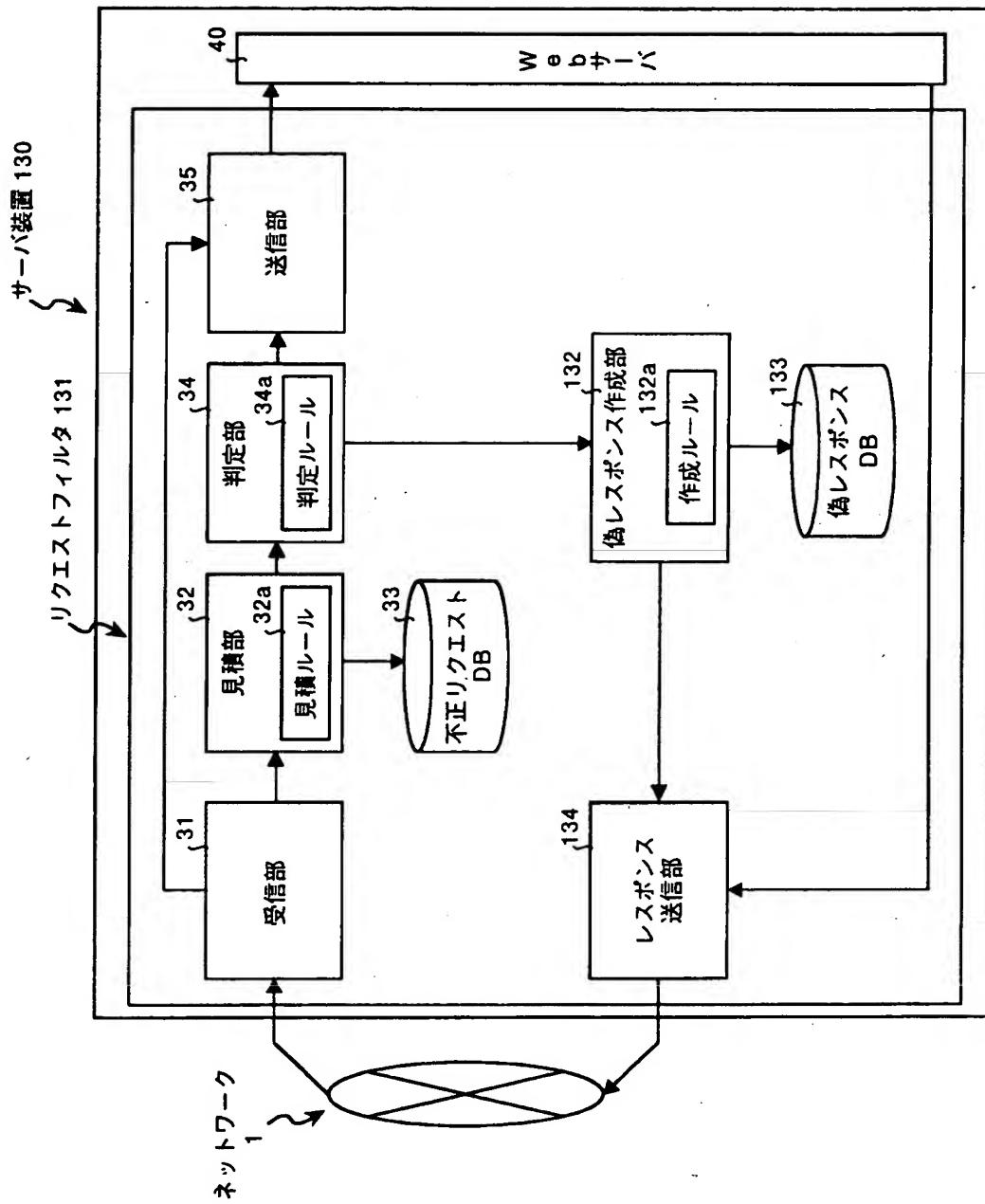
【図13】

本実施の形態7に係るサーバクライアントシステムの構成を示すブロック図



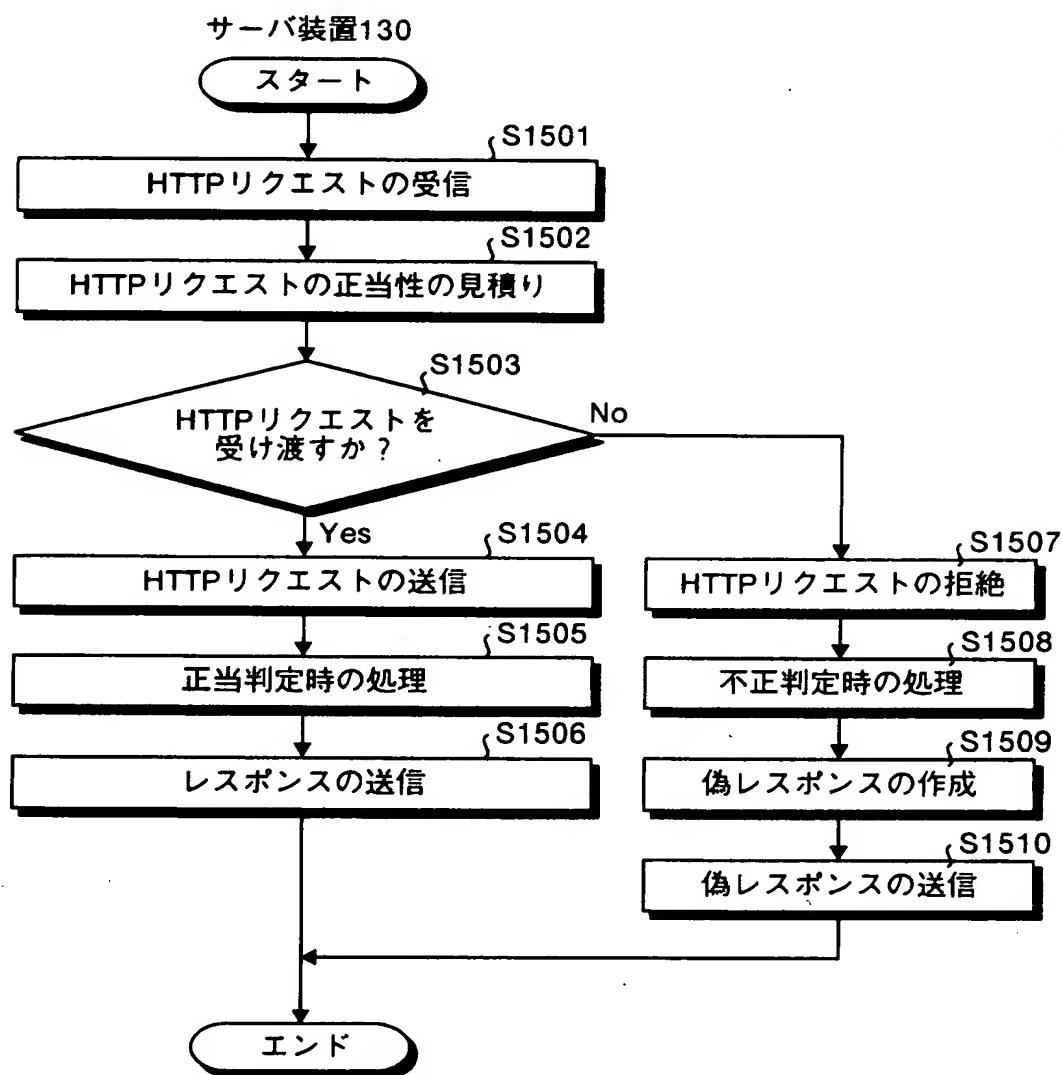
【図14】

本実施の形態8に係るサーバクライアントシステムの構成を示すプロック図



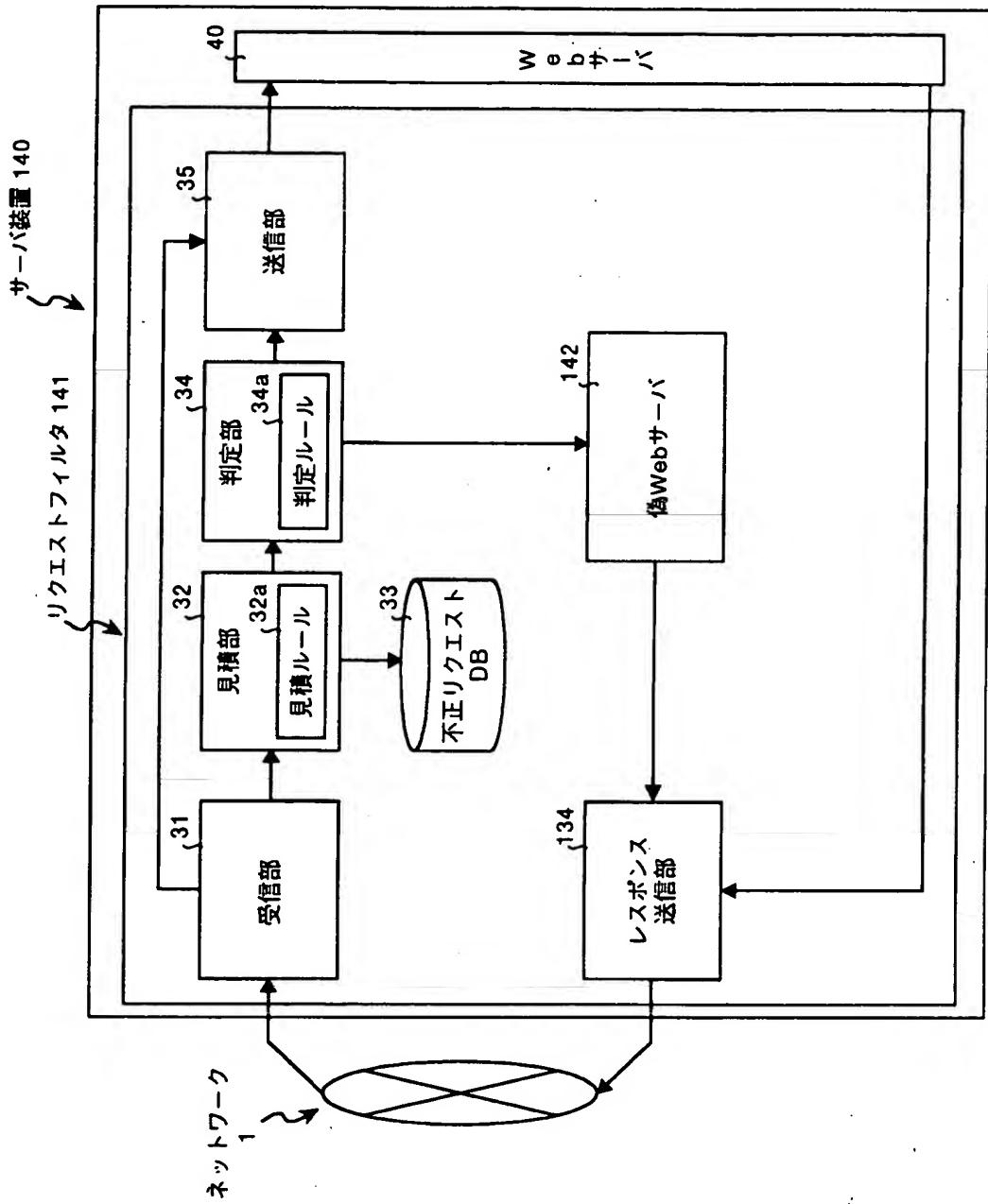
【図15】

本実施の形態8によるフィルタリングの処理手順を示すフローチャート



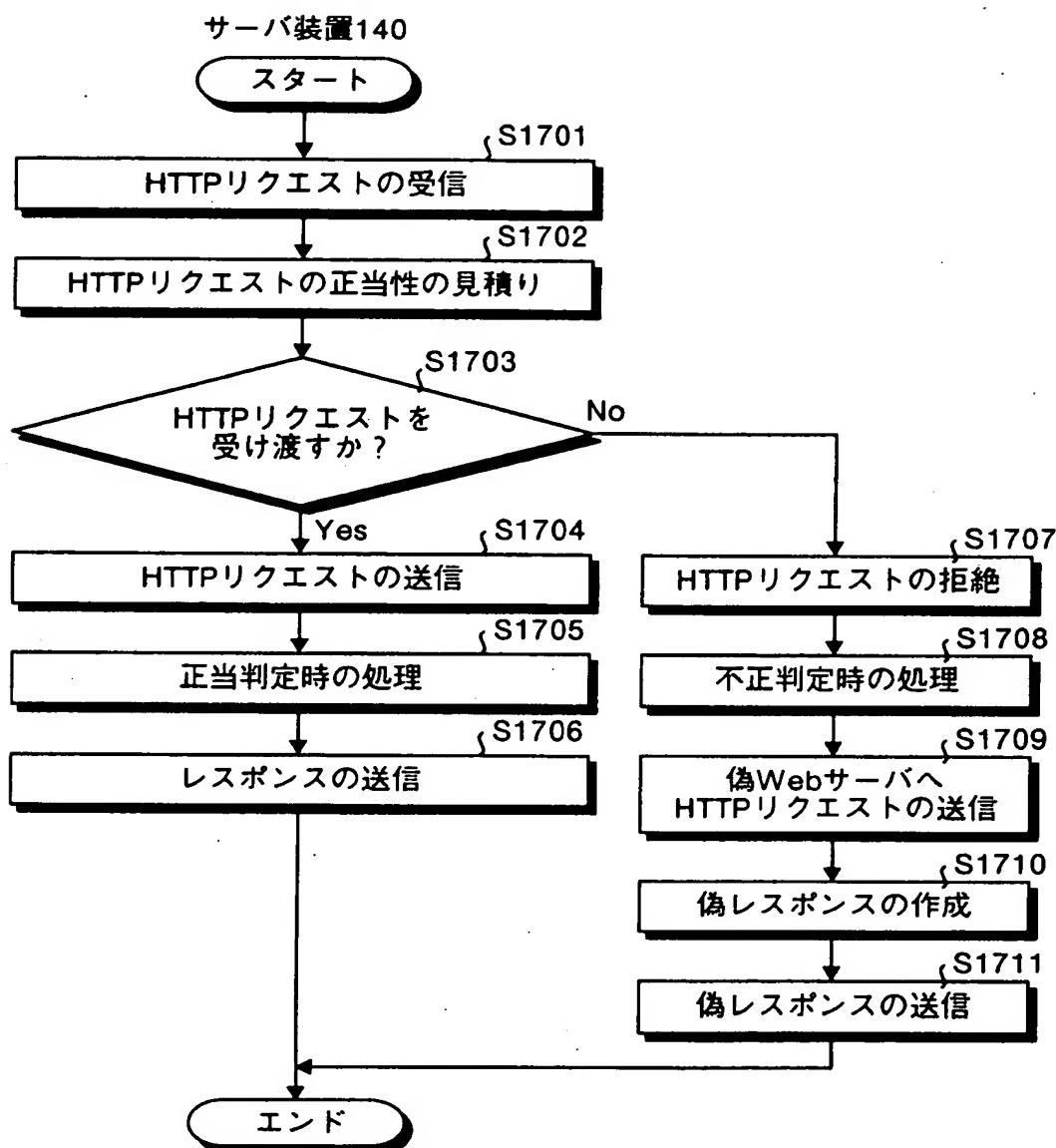
【図16】

本実施の形態9に係るサーバクライアントシステムの構成を示すブロック図



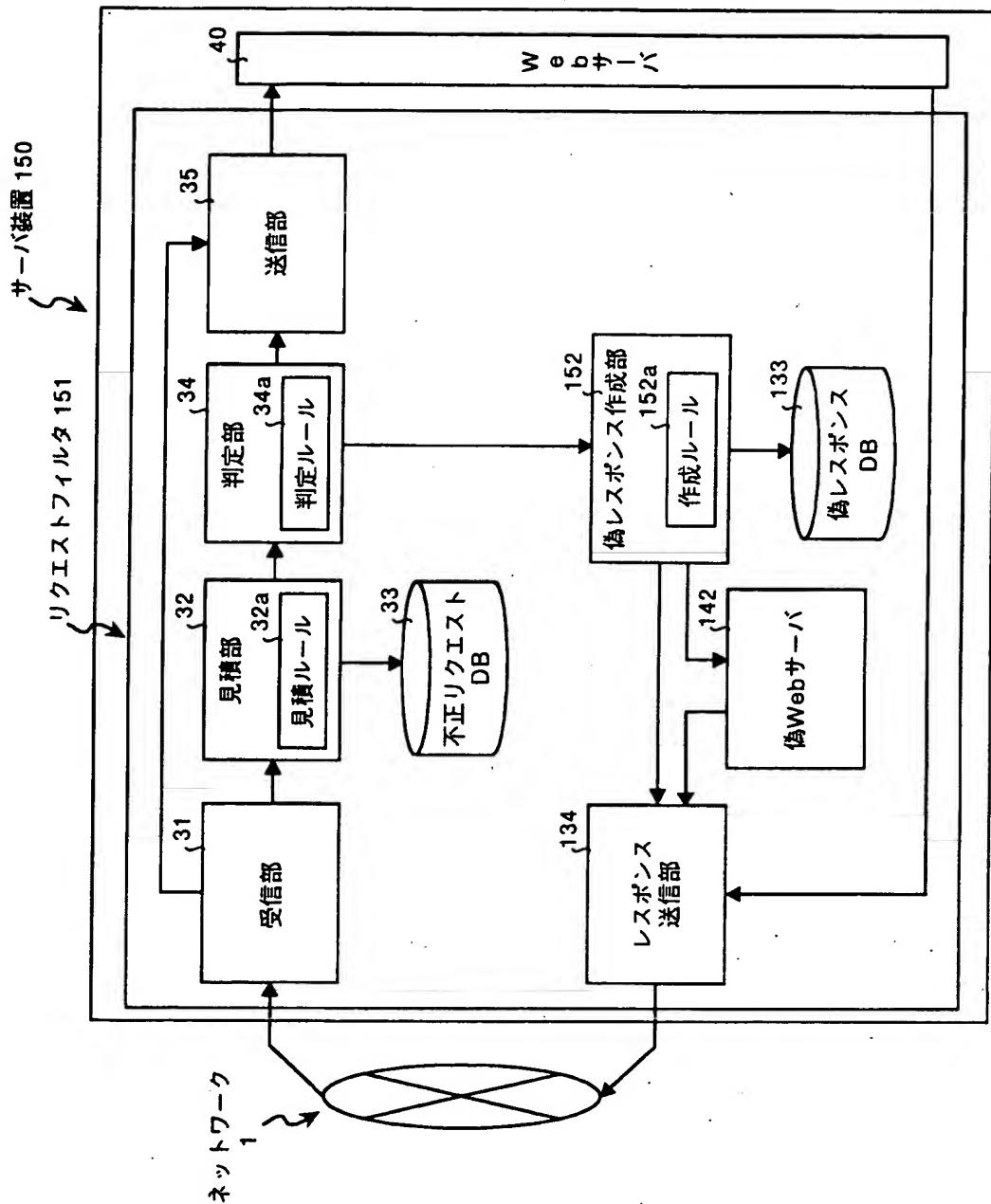
【図17】

本実施の形態9によるフィルタリングの処理手順を示すフローチャート



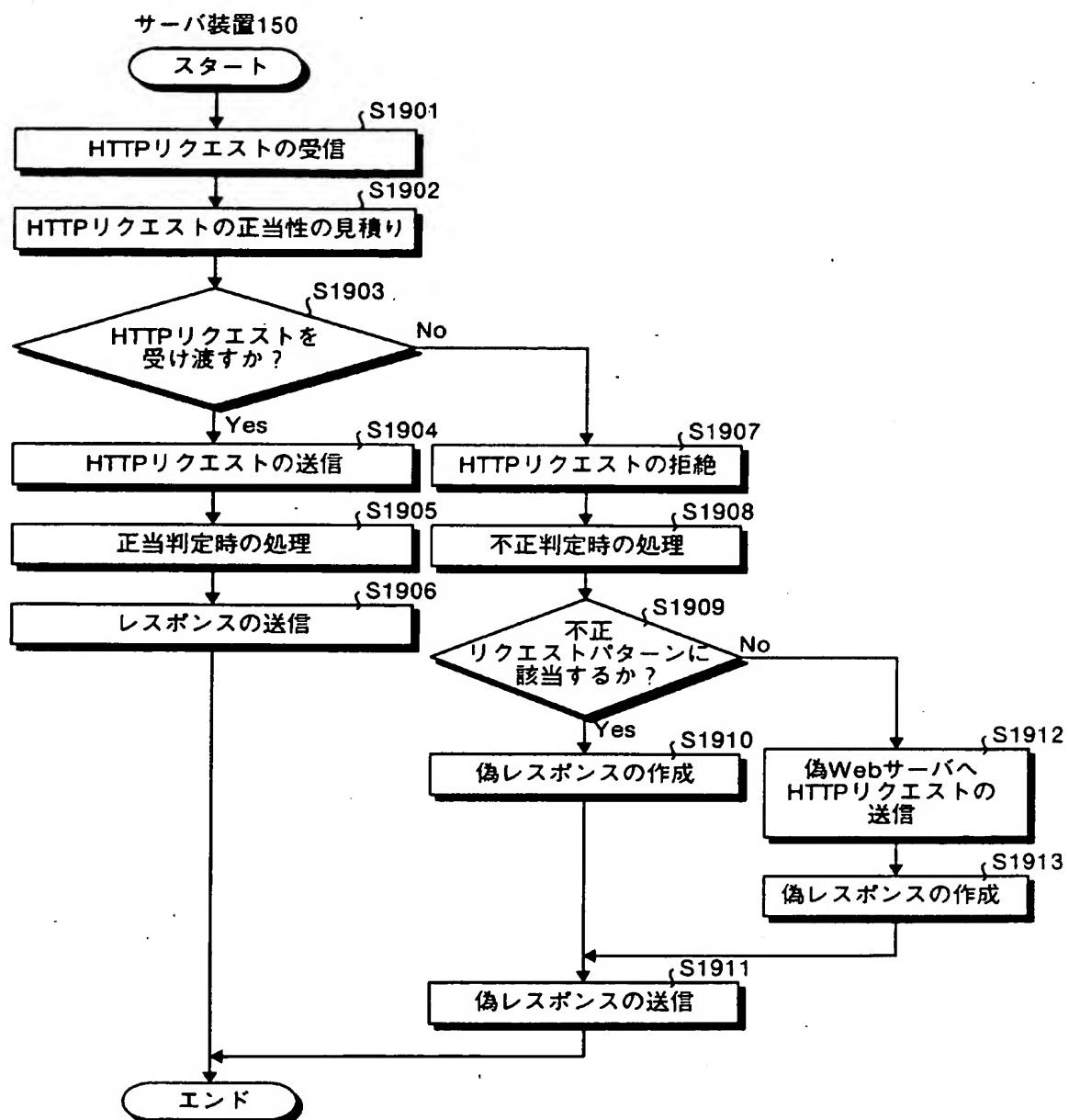
【図18】

本実施の形態10に係るサーバクライアントシステムの構成を示すブロック図



【図19】

本実施の形態10によるフィルタリングの処理手順を示すフローチャート



【書類名】 要約書

【要約】

【課題】 不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御すること。

【解決手段】 Webサーバ40に対する不正アクセスのパターンを格納した不正リクエストDB（データベース）33と、不正リクエストDB33に格納された不正アクセスのパターンおよび所定の見積ルール32aに基づいてクライアント装置10からのアクセス要求の正当性を見積もる見積部32と、見積部32による見積結果および所定の判定ルール34aに基づいてアクセス要求をWebサーバ40に受け渡すか否かを判定する判定部34とを備える。

【選択図】 図1

出願人履歴情報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号  
氏 名 富士通株式会社